

4 Ports ADSL2/2+ Router

User Manual

FOR ANNEX A/B

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All product, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a residential environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment ON and OFF, the user is encouraged to try to reduce the interference by one or more of the following measures:

- Adjust or relocate the receiving antenna
- Increase the separation between the equipment or device
- Consult a dealer or an experienced technician for assistance

CE Declaration of Conformity

This is to certify that this device complies the essential protection requirements of the European Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22). Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Contents

CHAPTER 1 INTRODUCTION.....	1
1.1 Features.....	2
1.2 Scope.....	5
1.3 Audience	6
1.4 Document Structure	7
1.5 System Requirement	8
1.6 Packet Contents	9
 CHAPTER 2 KNOWING THE 4 PORTS ADSL2/2+ ROUTER	10
2.1 Front Panel	10
2.2 Back Panel.....	11
2.3 Connection Mechanism:	12
 CHAPTER 3 SETTING UP THE TCP/IP IN WINDOWS.....	14
3.1 Windows ME / 98.....	15
3.2 Windows 2000	16
3.3 Windows XP	17
3.4 Checking TCP/IP Configuration.....	18
 CHAPTER 4 DEVICE ADMINISTRATION	21
4.1 Login	21
4.2 EZ SETUP	24
4.3 CONFIG.....	35
4.3.1 CONFIG - WAN Setup.....	36
4.3.1.1 CONFIG - WAN Setup – New Connection	37
4.3.1.1.1 New Connection - PPPoE Connection Setup.....	38
4.3.1.1.2 New Connection - PPPoA Connection Setup.....	41
4.3.1.1.3 New Connection - Static Connection Setup	43
4.3.1.1.4 New Connection - DHCP Connection Setup	45
4.3.1.1.5 New Connection - Bridge Connection Setup.....	47
4.3.1.1.6 New Connection - CLIP Connection Setup	49
4.3.1.2 CONFIG - WAN Setup - Modem	51
4.3.2 CONFIG - LAN Setup	52
4.3.2.1 LAN Setup - LAN Configuration.....	53
4.3.2.1.1 LAN Configuration - Unmanaged	54
4.3.2.1.2 LAN Configuration – Obtain an IP Address Automatically.....	55

4.3.2.1.3 LAN Configuration – PPP IP Address.....	56
4.3.2.1.4 LAN Configuration – Use The Following Static IP Address	57
4.3.3 LAN Setup - Firewall/NAT Services	59
4.3.4 CONFIG – Save All.....	60
4.4 ADVANCED	61
4.4.1 ADVANCED - UPnP.....	62
4.4.2 ADVANCED - SNTP	63
4.4.3 ADVANCED - SNMP.....	64
4.4.4 ADVANCED - IP QoS	66
4.4.5 ADVANCED - Port Forwarding	68
4.4.6 ADVANCED - IP Filters.....	71
4.4.7 ADVANCED - LAN Clients	73
4.4.8 ADVANCED - LAN Isolation	74
4.4.9 ADVANCED - Bridge Filters.....	75
4.4.10 ADVANCED – Web Filters	77
4.4.11 ADVANCED - Multicast.....	78
4.4.12 ADVANCED – Static Routing.....	79
4.4.13 ADVANCED – Dynamic Routing.....	80
4.4.14 ADVANCED – Access Control	81
4.4.15 ADVANCED – Save All	82
4.5 TOOLS.....	83
4.5.1 TOOLS - System Commands.....	84
4.5.2 TOOLS - Remote Log.....	86
4.5.3 TOOLS - User Management.....	87
4.5.4 TOOLS - Update Gateway.....	88
4.5.5 TOOLS - Ping Test.....	90
4.5.6 TOOLS - Modem Test.....	91
4.5.7 TOOLS – Save All.....	92
4.6 STATUS	93
4.6.1 STATUS - Network Statistics	94
4.6.1.1 STATUS - Network Statistics - Ethernet	95
4.6.1.2 STATUS - Network Statistics - DSL	96
4.6.2 STATUS – Connection Status.....	97
4.6.3 STATUS - DHCP Clients.....	98
4.6.4 STATUS - Modem Status.....	99
4.6.5 STATUS - Product Information	100
4.6.6 STATUS - System Log.....	101
APPENDIX A: ROUTER TERMS.....	102

APPENDIX B: HELPS	104
APPENDIX C: FREQUENTLY ASKED QUESTIONS	109
APPENDIX D: TROUBLESHOOTING GUIDE.....	111
APPENDIX E: UPNP SETTING ON WINDOWS XP	114
APPENDIX F: GLOSSARY	118

Chapter 1 Introduction

Congratulations on your purchase of this outstanding 4 Ports ADSL2/2+ Router. This device is a Four Ports Ethernet ADSL2/2+ Router combines an “Always-On” high speed Asymmetric Digital Subscriber Line (ADSL/ADSL2/ADSL2+) connection to the Telephone Line, and four 10/100BASE-T Ethernet Switch connection to a host PC or other Ethernet device to enable the widest array of host connectivity. This 4 Ports ADSL2/2+ Router is specially designed for residential, industries and SOHO users.

ADSL2/2+ is a transmission technology used to carry user data over a single twisted-pair line between the Central Office and the Customer Premises. The downstream data rates can go up to 24 Mbps and the upstream data rates can go up to 1Mbps with length reach up to 22Kft. This asymmetric nature lends itself to applications such as Internet access and video delivery.

With minimum setup, you can install and use the router within minutes.

1.1 Features

■ The 4 Ports ADSL2/2+ Router provides the following features:

- Compliant to ANSI T1.413 Issue 2, ITU-T G.992.1, ITU-T G.992.2, ITU-G.992.3, ITU 992.4, ITU G.992.5 and READSL2 standards. Support all Digital Loop ITU G.992.3 annex I and J specifications. Fully compliant with Annex A/B/B (U-R2) ADSL specifications.
- Downstream and Upstream data rates up to 24Mbps and 1Mbps.
- Support RFC 1483 Bridge/Routing over ATM over ADSL.
- Support PPPoE, PPPoA and IPoA Routing ATM over ADSL.
- ATM Layer with Traffic Shaping QoS support (UBR, CBR, VBR-rt, VBR-nt).
- Support UPnP functionality.
- Web-based setup for installation and management.
- Built-in 4*10/100 Mbps Fast Ethernet Switch port for LAN connection.
- Compliant with IEEE 802.3/802.3u and auto-negotiation.
- Support full-duplex 802.3 flow control.
- Support IP Filtering, MAC Filtering, Web Filtering and IPSec Pass-Through security functionality.
- Support Dying Gasp functionality (Optional).
- Flash memory for firmware upgrade.
- Hardware Reset button for fast default setting recovery.
- HTTP Web-Based Management/Configuration.
- LEDs indicator indicates connection status.

■ ADSL Standards

- Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
- ITU G.992.3, ITU G.992.5 and READSL2 ADSL2/2+ standards compliant.
- Downstream and Upstream data rates up to 24Mbps and 1Mbps.
- Reach length up to 22Kft.
- Support Dying Gasp functionality (Optional).

■ **ATM Protocols**

- Support ATM ALL0, ALL2 & ALL5.
- Support up to 16PVCs.
- Support ATM UBR, CBR, VBR-rt and VBR-nt Traffic Shaping QoS.
- Support OAM F4/F5 Loop Back.
- Support PPPoA (RFC2364).
- Support PPPoE (RFC2516).
- Router/Bridged Ethernet over ATM (RFC2864 / RFC1483).
- Classical IP over ATM (RFC2225 / RFC1577).

■ **Router Mode**

- IP Routing – RIPv1 and RIPv2.
- Static Routing.
- DHCP Server, Relay and Client.
- Support DNS Relay/Server.
- Support DMZ functionality.
- Support NAT and NAPT (PAT) functionality with extensive ALG supported.
- Support IPSec, L2TP, PPTP Pass-Through.
- Support VPN Pass-Through.
- Support SNMP functionality.
- Support ICMP and IGMP.
- Support PAP and CHAP PPP Authentication.

■ **Bridge Mode**

- Support Transparent Bridging (IEEE 802.1D).Support RFC 2684/1483 Bridged.**Firewall**
- Built in Firewall functionality.
- Support IP Filtering.
- Support MAC Filtering.
- Support Web Filtering.
- IPSec Pass-Through.
- Protection against IP and MAC address spoofing.

■ **UPnP**

- Support UPnP functionality.

■ Ethernet Standards

- Built-in 4 Ports 10/100Mbps Ethernet Switch which compliant with IEEE 802.3x standards
- Automatic MDI/MDI-X crossover for 100BASE-TX and 10BASE-T ports.
- Auto-negotiation and speed-auto-sensing support.
- Port based VLAN supported in any combination.

■ Web-Based Management

- Web-based Configuration / Management.
- Remote / Local Management / Configuration.
- Firmware upgrade and Reset to default via Web management.
- Telnet, TFTP and FTP Management / Configuration.
- SNMP MIB-II.
- Restore factory default setting via Web or hardware reset button.
- WAN and LAN connection statistics.
- Configuration of static routes and routing table, NAT/NAPT and VCs.
- Support Password Authentication.

1.2 Scope

This document provides the descriptions and usages for the 4 Ports ADSL2/2+ Router's Web pages that are used in the configuration and setting process. Both basic and advanced descriptions and concepts are discussed. To help the reader understand more about these Web pages, some questions and answers (Q&A) are appended after the definition of each Web page along with the appendices at the end of the guide.

1.3 Audience

This document is prepared for use by those customers who purchase the 4 Ports ADSL2/2+ Router and using the provided or embedded firmware. It assumes the reader has a basic knowledge of ADSL/ADSL2/ADSL2+ and networking.

1.4 Document Structure

- Chapter 1: Introduction, provides a brief introduction to the product and user guide.
- Chapter 2: Knowing The 4 Ports ADSL2/2+ Router, provides device specifications and hardware connection mechanism.
- Chapter 3: Setting Up TCP/IP In Windows, provides Windows system Network's configurations.
- Chapter 4: Device Administration, describes the pages found under the Admin menu. These pages allow the user to view, change, edit, update, and save the 4 Ports ADSL2/2+ Router's configurations or settings.
- Appendix A: Router Terms, provides an introduction to basic Router Terms.
- Appendix B: Helps, provides Help description for Firewall, Bridge Filters, LAN Clients and PPP connection.
- Appendix C: Frequently Asked Questions, is a compilation of useful questions regarding the 4 Ports ADSL2/2+ Router.
- Appendix D: Troubleshooting Guide, is a compilation of questions and answers relating to common problems dealing with Windows networking and the 4 Ports ADSL2/2+ Router configurations.
- Appendix E: UPnP Setting, provides UPnP configurations procedures under Windows XP.
- Appendix F: Glossary, provides definitions of terms and acronyms of this 4 Ports ADSL2/2+ Router.

1.5 System Requirement

Check and confirm that your system confirm the following minimum requirements:

- Personal computer (PC/Notebook).
- Pentium II compatible processor and above.
- Ethernet LAN card installed with TCP/IP protocol.
- USB Port (Optional)
- 64 MB RAM or more.
- 50 MB of free disk space (Minimum).
- Internet Browser.
- CD-ROM Drive.

1.6 Packet Contents

The 4 Ports ADSL2/2+ Router package contains the following items :

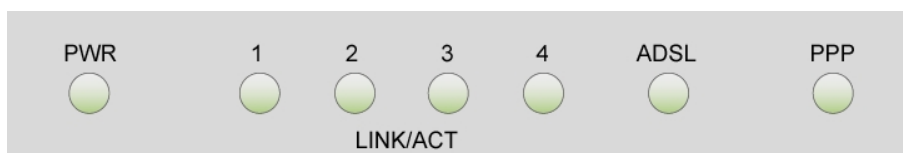
- One 4 Ports ADSL2/2+ Router
- One Power Adapter
- One RJ-11 ADSL Cable
- One CAT-5 Ethernet Cable
- One CD-ROM (Driver / Manual / Quick Setup Guide)

If any of the above items are damaged or missing, please contact your dealer immediately.

Chapter 2 Knowing The 4 Ports ADSL2/2+ Router

2.1 Front Panel:

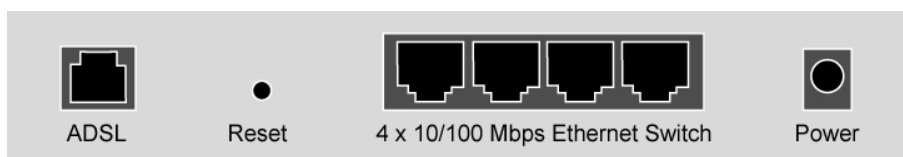
The 4 Ports ADSL2/2+ Router's LEDs indicators display information about the device's status.



PWR	Lights up when 4 Ports ADSL2/2+ Router is powered on.
1 LINK/ACT	Blinking when 4 Ports ADSL2/2+ Router is Sending/Receiving data.
2 LINK/ACT	Blinking when 4 Ports ADSL2/2+ Router is Sending/Receiving data.
3 LINK/ACT	Blinking when 4 Ports ADSL2/2+ Router is Sending/Receiving data.
4 LINK/ACT	Blinking when 4 Ports ADSL2/2+ Router is Sending/Receiving data.
ADSL	Blinking when 4 Ports ADSL2/2+ Router is ready.
	Lights up when a successful ADSL connection is established.
PPP	Lights up when a PPP connection is established.

2.2 Back Panel:

The back panel of the 4 Ports ADSL2/2+ Router contains ADSL, Ethernet Switches, Reset and Power Adapter connection.



ADSL	Port for connecting to the ADSL2/2+ Service Provider.
Ports 1~4	Four 10/100Mbps Ethernet Ports for connecting to the network devices
RESET	Restore the 4 Ports ADSL2/2+ Router to factory default setting.
POWER	12V DC/1A or 9V AC/1A Power adapter connector.



All the Ethernet port of the 4 Ports ADSL2/2+ Router supports auto-crossover capability.



RESET Button:

Reboot & Restore the 4 Ports ADSL2/2+ Router to factory defaults.

Resetting Factory Defaults:

The reboot and restore to factory defaults feature will set the device to its factory default configuration by resetting the 4 Ports ADSL2/2+ Router.

To Reset the 4 Ports ADSL2/2+ Router:

- Ensure that the device is powered on.
- Press the Reset button for 10~15 seconds and release. Wait for 30 seconds after release the Reset button. Do not power off the device during the reset process.
- The default settings are now restored after 30 seconds.

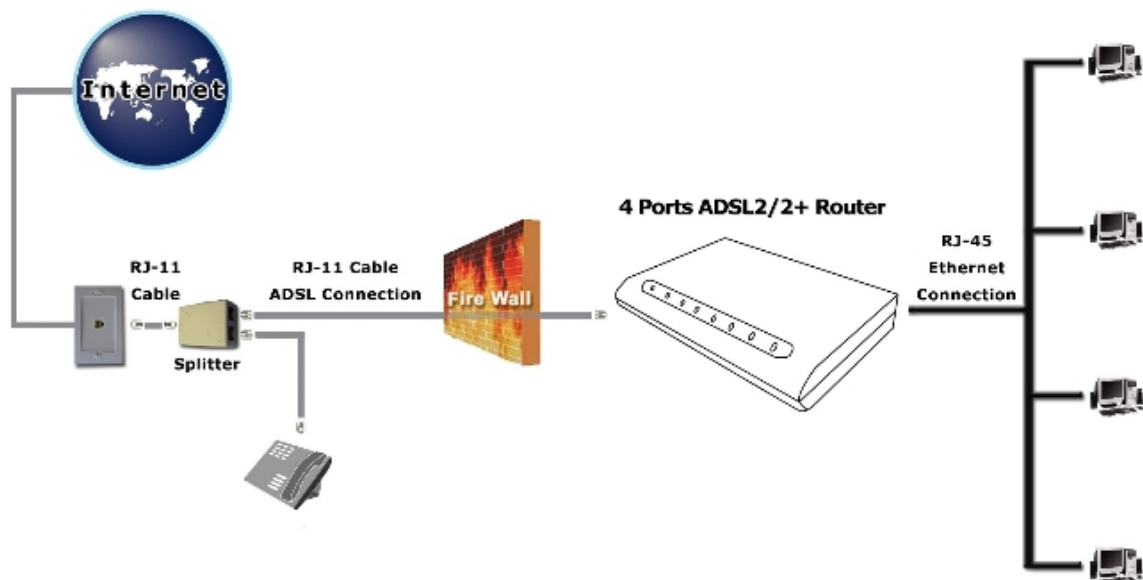
2.3 Connection Mechanism:

This section describes the hardware connection mechanism of 4 Ports ADSL2/2+ Router on your Local Area Network (LAN) connected to the Internet, how to configure your 4 Ports ADSL2/2+ Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 4 Ports ADSL2/2+ Router:

1. A computer/notebook which must have an installed Ethernet Adaptor and an Ethernet Cable,
2. ADSL/ADSL2/ADSL2+ service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your 4 Ports ADSL2/2+ Router to the Internet:
 - a. VPI/VCI parameters
 - b. Multiplexing Method or Protocol Type
 - c. Host and Domain Names
 - d. ISP Login Name and Password
 - e. ISP Domain Name Server (DNS) Address
 - f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 4 Ports ADSL2/2+ Router.



Following are the steps to properly connect your 4 Ports ADSL2/2+ Router:

1. Turn off your computer/notebook.
2. Connect the ADSL port of your 4 Ports ADSL2/2+ Router to the wall jack of the ADSL/ADSL2/ADSL2+ Line with a RJ-11 cable.
3. Connect the Ethernet cable (RJ-45) from your 4 Ports ADSL2/2+ Router (Switch) to the Ethernet Adaptor in your computer.
4. Connect the Power adaptor to the 4 Ports ADSL2/2+ Router and plug it into a Power outlet.



***The Power light will lit after turning on the 4 Ports ADSL2/2+ Router.
Auto and self-diagnostic process might turn the LED indicators ON and
OFF during the process.***

5. Turn on your computer.
6. Refer to the next section to setup or configure your system's Network Adaptor.

Chapter 3 Setting up the TCP/IP in Windows

The instruction in this chapter will help you configure your computers to be able to communicate with this 4 Ports ADSL2/2+ Router.

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer/notebook on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

The following description assumes 4 Ports ADSL2/2+ Router been set to factory default. (If not, please hold the reset button down for 5~10 seconds). The default of the 4 Ports ADSL2/2+ Router's LAN IP is **192.168.1.1**.

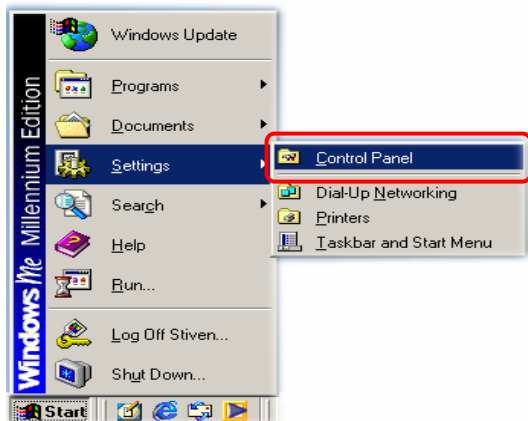
Follow the procedures below to set your computer/notebook function as a **DHCP Client**.



Restart and Reboot your Windows system might be necessary after setting your computer function as a DHCP Client. In order to properly activate your choice, click "OK" to restart your Windows system.

3.1 Windows ME / 98

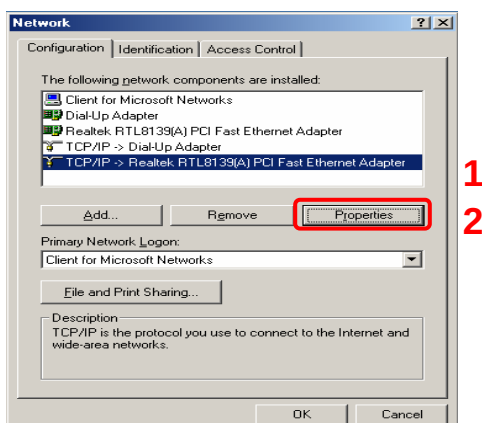
Step 1: Click **Start**→**Settings**→**Control Panel**.



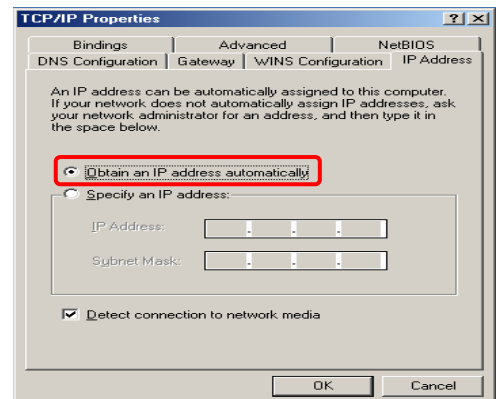
Step 2: Double-click the **Network** icon.



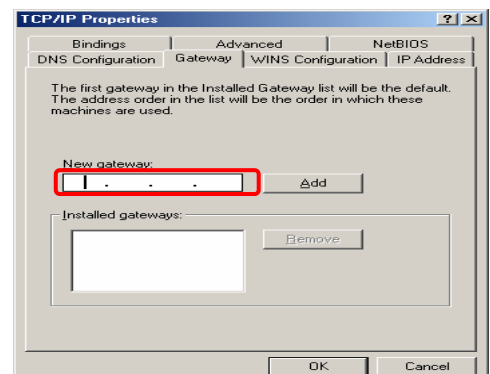
Step 3: Go to Configuration icon, select network adapter installed and click **Properties**.



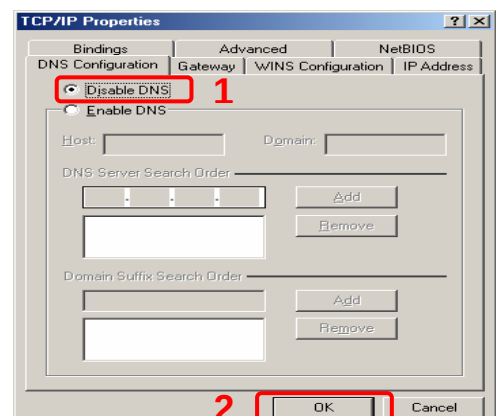
Step 4: Go to IP Address icon and select **Obtain an IP address**.



Step 5: Go to Gateway icon and erase all previous setting.

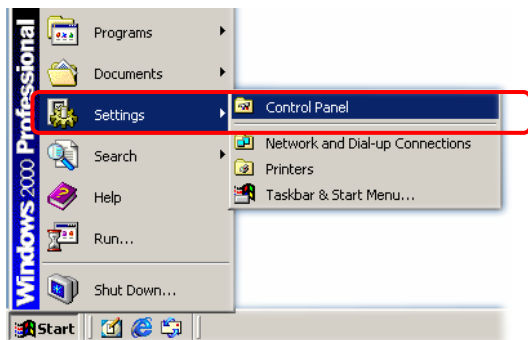


Step 6: Go to DNS Configuration icon, select **Disable DNS** and click **OK**.



3.2 Windows 2000

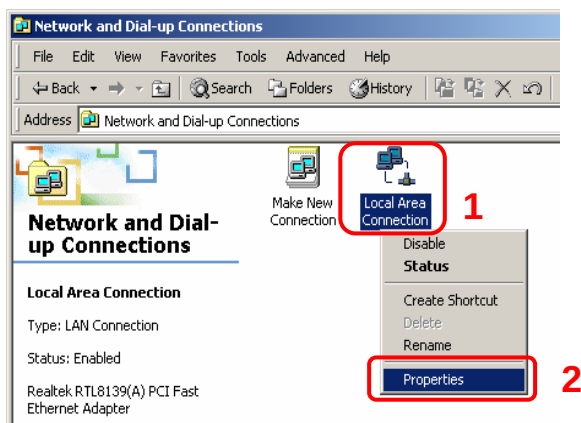
Step 1: Click **Start**→**Settings**→**Control Panel**.



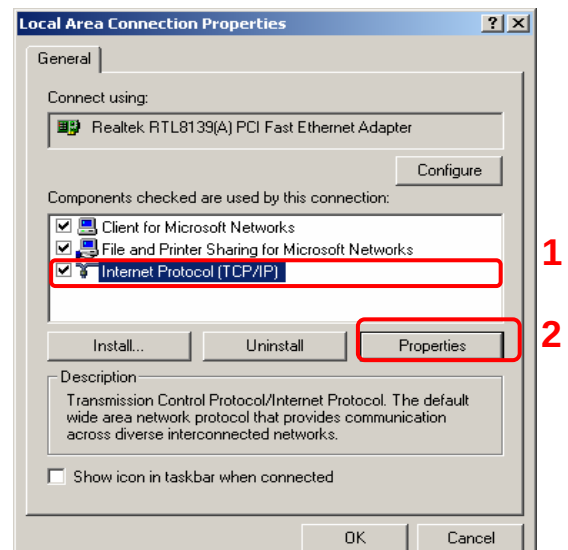
Step 2: Double-click the **Network and Dial-up Connections**.



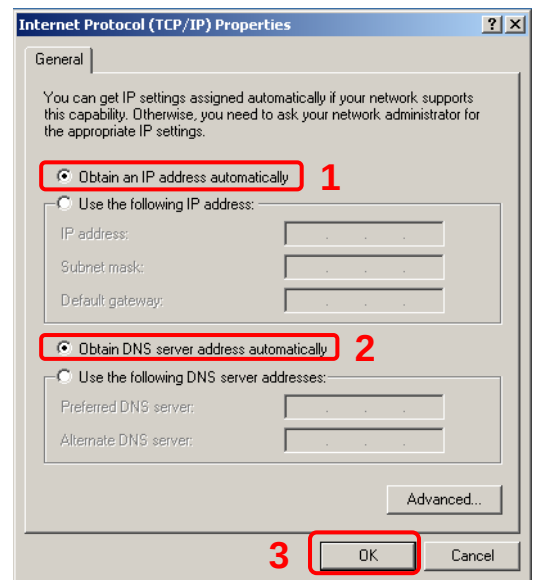
Step 3: Right Click the **Local Area Connection** and select **Properties**.



Step 4: Select **Internet Protocol (TCP/IP)** and click **Properties**.

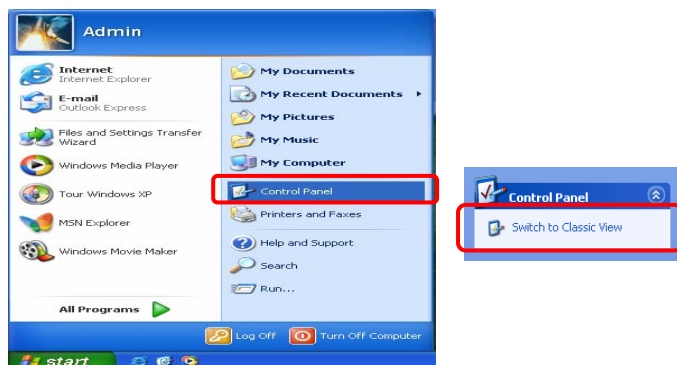


Step 5: Select **Obtain an IP address automatically** and **DNS server address automatically**. Then, click **OK**.

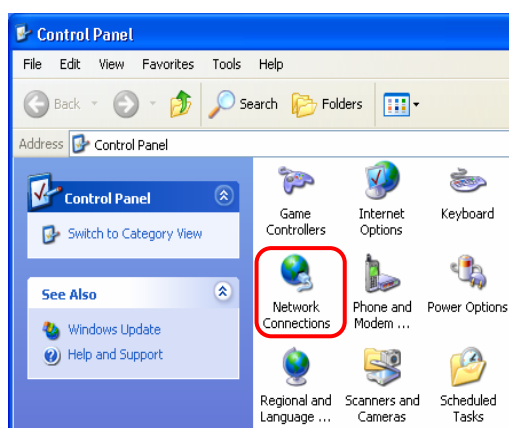


3.3 Windows XP

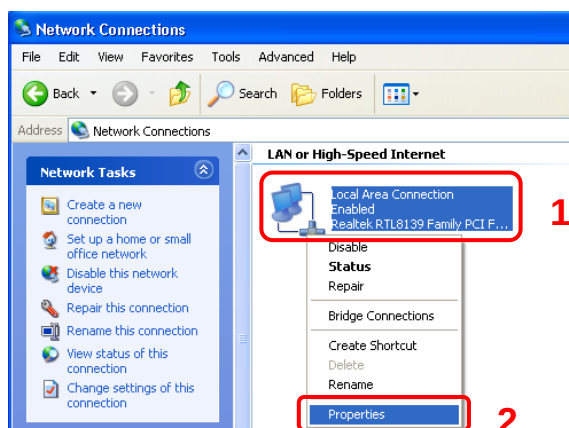
Step 1: Click **Start**→**Control Panel**→**Classic View**.



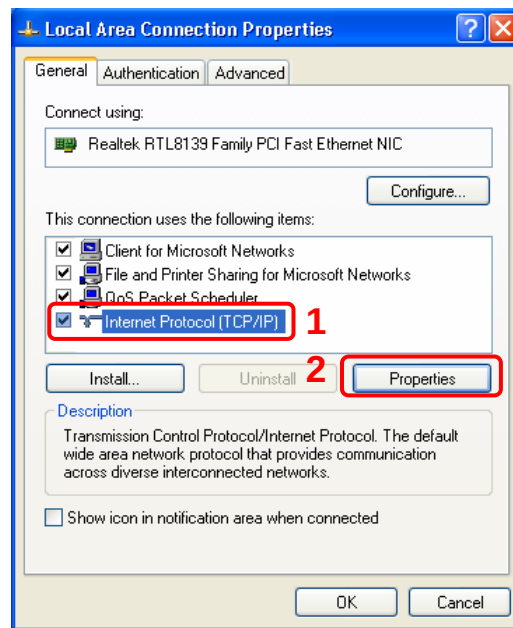
Step 2: Double-click the **Network Connections**.



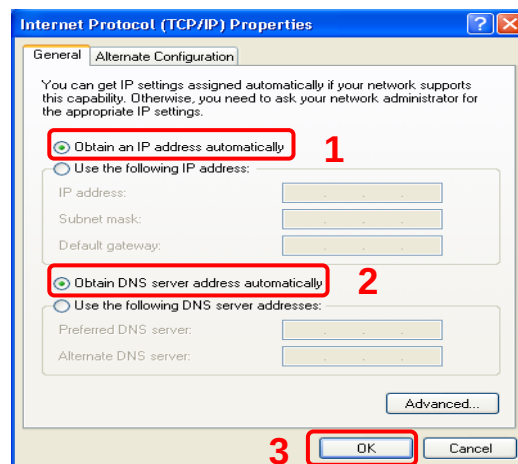
Step 3: Right Click on the **Local Area Connection** and select **Properties**.



Step 4: Go to **General** icon, select **Internet Protocol (TCP/IP)** and click **Properties**.



Step 5: Go to **General** icon, select **Obtain an IP address automatically** and **DNS server address automatically**. Then, click **OK**.

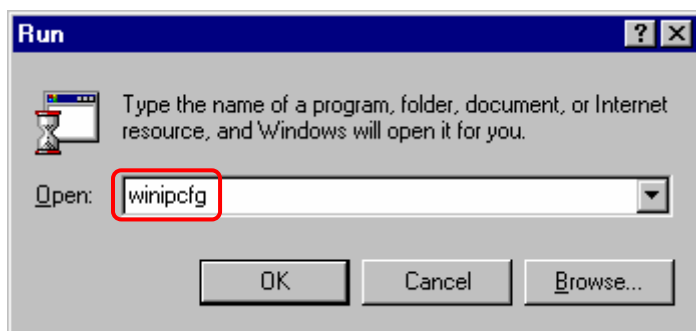


3.4 Checking TCP/IP Configuration

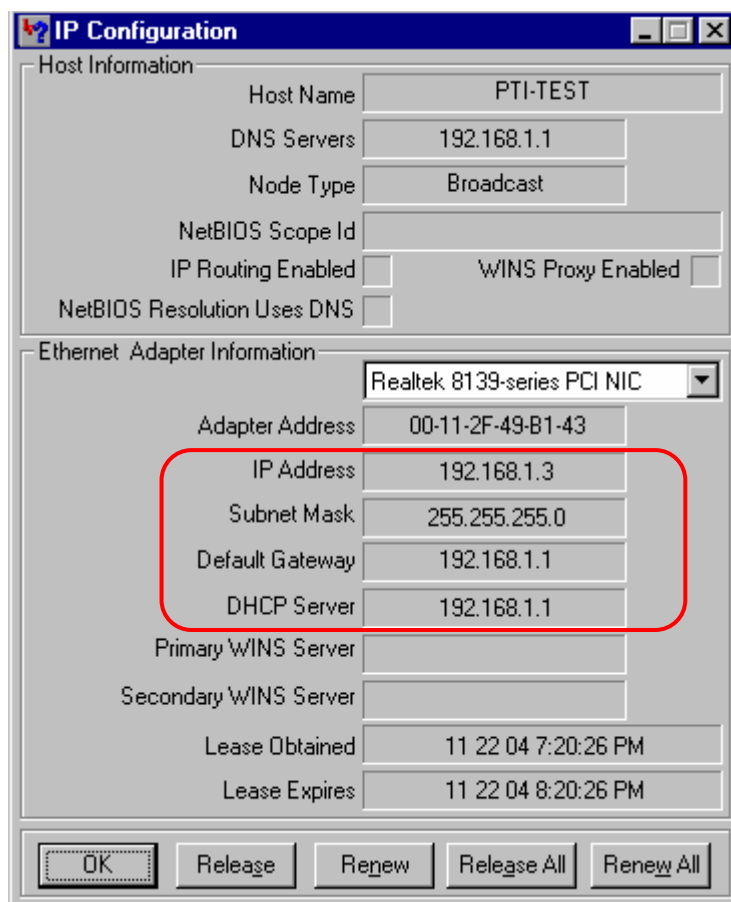
After your PC is configured and the system has rebooted, you can check the TCP/IP configuration using the following utility provided by your Windows system:

A. Windows 98/ME:

1. Click on “Start” and “Run”.
2. In the open field, enter “winipcfg”, then press “OK”.



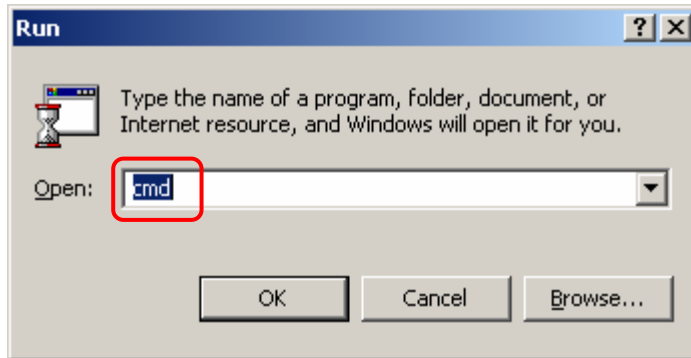
3. All the Ethernet adapter information will be shown in the appears Windows. Check if you can get the following setting:



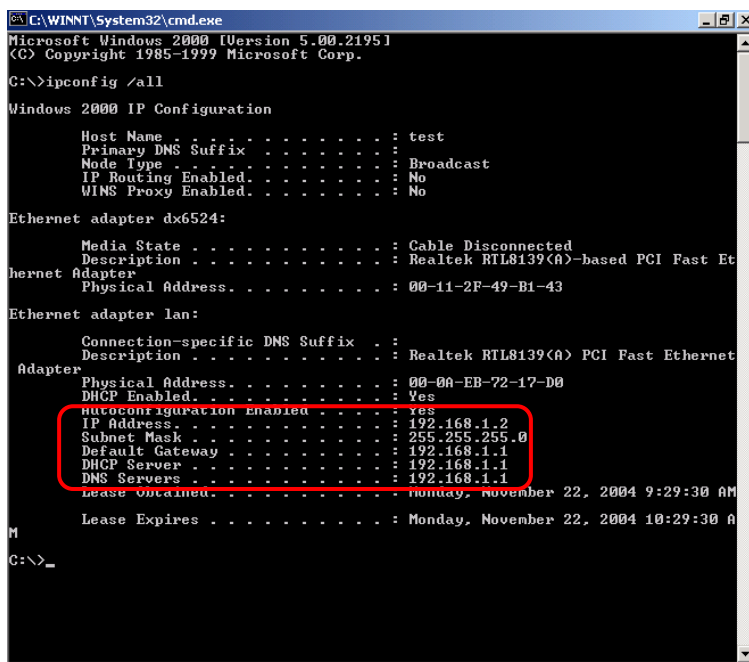
- The IP Address as 192.168.1.x
 - The Subnet Mask as 255.255.255.0
 - The Default Gateway as 192.168.1.1
4. Type “OK” to end up the process.

B. Windows 2000:

1. Click “Start” and “Run”.
2. In the open field, enter “cmd” then click “OK”.



3. In the command prompt, type “ipconfig /all”, then press “Enter”.

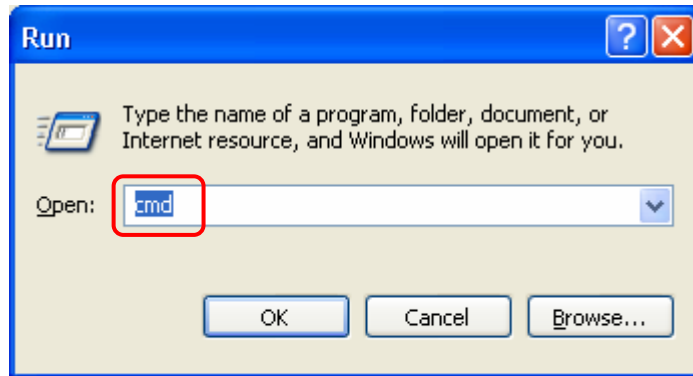


All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

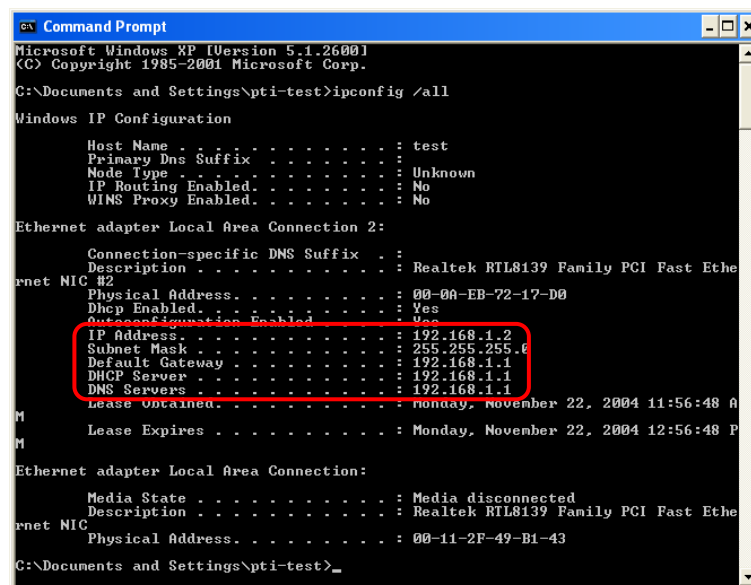
- The IP Address as 192.168.1.x
 - The Subnet Mask as 255.255.255.0
 - The Default Gateway as 192.168.1.1
4. Type “Exit” to end up the process.

C. Windows XP:

1. Click **“Start”** and **“Run”**.
2. In the open field, enter **“cmd”** then click **“OK”**.



3. In the command prompt, type **“ipconfig /all”**, then press **“Enter”**



All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

- IP address as **192.168.1.x**
 - The Subnet Mask as **255.255.255.0**
 - the default gateway as **192.168.1.1**
4. Type **“Exit”** to end up the process.

Chapter 4 Device Administration

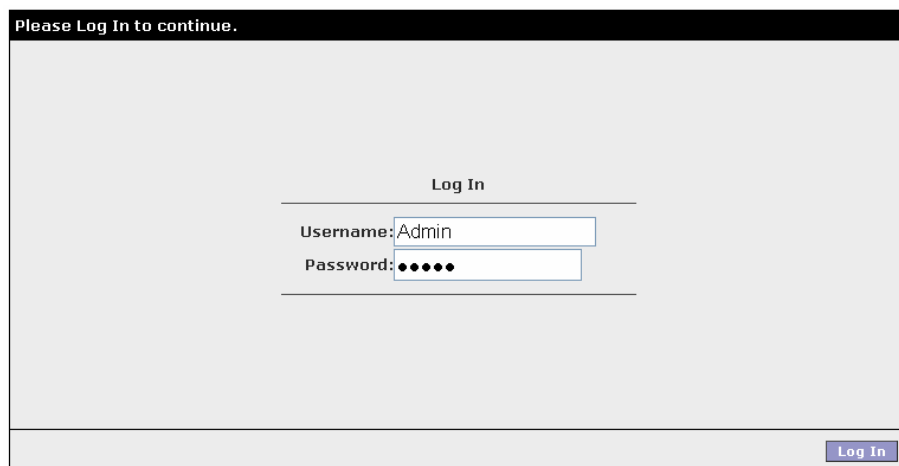
For your convenience, an Administrative Utility has been programmed into 4 Ports ADSL2/2+ Router. This chapter will explain all the functions in this utility. All the 4 Ports ADSL2/2+ Router based administrative tasks are performed through this web utility.

4.1 Login

To access the 4 Ports ADSL2/2+ Router Configuration screens, follow the following steps will enable you to log into the 4 Ports ADSL2/2+ Router:

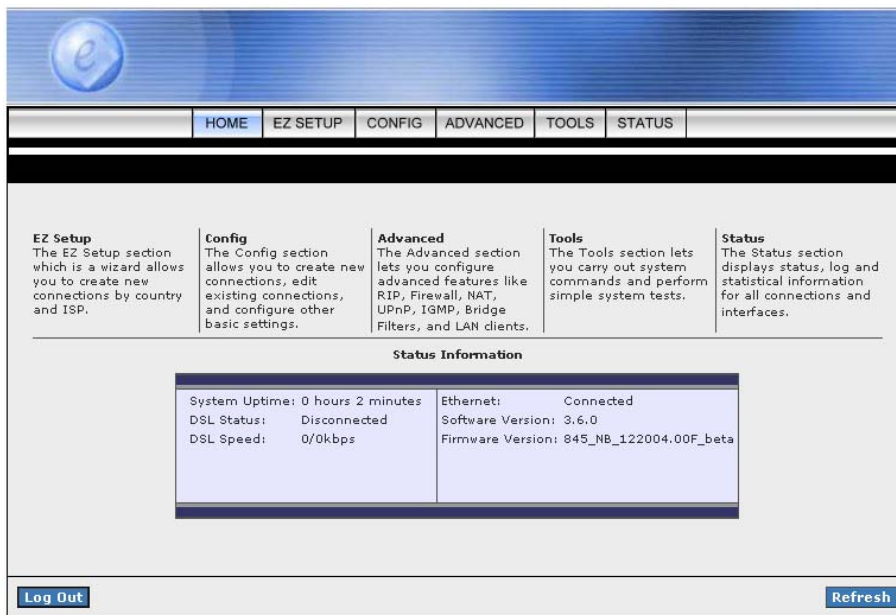
1. Launch the Web browser (Internet Explorer, Netscape, etc).
2. Enter the 4 Ports ADSL2/2+ Router default IP address (Default Gateway) <http://192.168.1.1> in the address bar then press Enter to Log in.
3. Entry of the username and password will be prompted. Enter the default login “**Username**” and “**Password**”: The default login Username of the administrator is “**Admin**”, and the default login Password is “**Admin**”.

■ **Note that the Username and Password are case sensitive.**



“**Username**” and “**Password**” can be changed after login. Refer to the **Tools** configuration section for further instruction.

Upon entering the address into the web browser, the configurable **HOME** page with all the device configuration information will pop up as shown in Figure below.

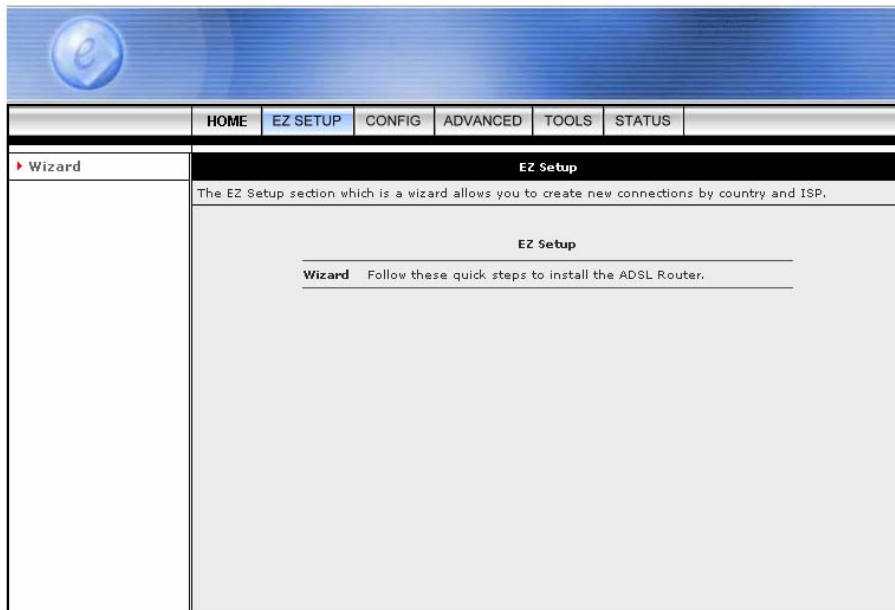


- **HOME:** The **Home** section show the current 4 Ports ADSL2/2+ Router's function information under different links.
- **EZ SETUP:** The **EZ Setup** is meant to help you install the 4 Ports ADSL2/2+ Router quickly and easily.
- **CONFIG:** The **Config** section allows you to create new connections, edit existing connections, and configure other basic settings.
- **ADVANCED:** The **Advanced** section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.
- **TOOLS:** The **Tools** section lets you carry out system commands and perform simple system tests.
- **STATUS:** The **Status** section displays status, log and statistical information for all connections and interfaces.

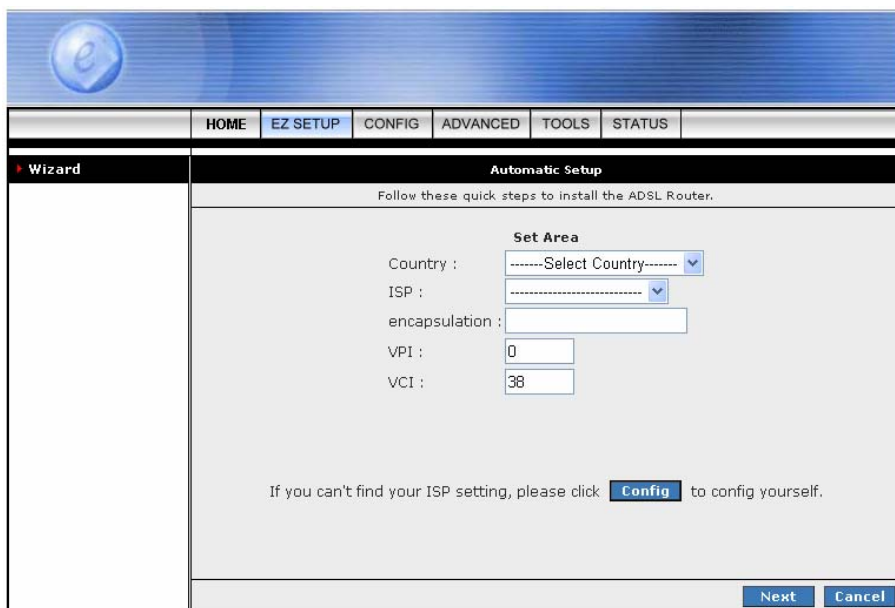
- **Status Information:** Shows the current device connection status.
 - ☑ **System Uptime:** This field displays the time of the 4 Ports ADSL2/2+ Router has been in operation.
 - ☑ **DSL Status:** Shows the 4 Ports ADSL2/2+ Router connection status.
 - ☑ **DSL Speed:** This field displays the 4 Ports ADSL2/2+ Router Downstream/Upstream data rate in Kbps
 - ☑ **Ethernet:** This field displays the link up or down for the Ethernet connection.
 - ☑ **USB:** This field displays the link up or down for the USB connection (Optional).
 - ☑ **Software Version:** This field displays the 4 Ports ADSL2/2+ Router's software version.
 - ☑ **Firmware Version:** This field displays the 4 Ports ADSL2/2+ Router's firmware version.
- **Log Out:** Click to Log Out the Administration configuration page.
- **Refresh:** Click to Refresh current page.

4.2 EZ SETUP

The **EZ SETUP** is meant to help you install the 4 Ports ADSL2/2+ Router quickly and easily.



Click on “**Wizard**” and the following screen will pop-up. Follow the **Steps** describe below to complete your installation.



STEP 1. Select your country from the **Country** list and the ADSL service provider from the **ISP** List (If there are more than two ISP in your country) and note the “**Encapsulation**” type and “**VPI/VCI**” setting.

The screenshot shows the 'Automatic Setup' wizard for an ADSL router. The interface has a blue header with a logo and a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. The 'EZ SETUP' tab is active, and the 'Wizard' section is expanded. The main area is titled 'Automatic Setup' and contains the text 'Follow these quick steps to install the ADSL Router.' Below this is the 'Set Area' section with the following fields:

- Country : Taiwan (dropdown menu)
- ISP : Hinet (dropdown menu)
- encapsulation : PPPoE LLC (text field)
- VPI : 0 (text field)
- VCI : 33 (text field)

At the bottom of the 'Set Area' section, there is a note: 'If you can't find your ISP setting, please click **Config** to config yourself.' Below the note are two buttons: 'Next' and 'Cancel'.



Click “Config” if you can’t find any available parameters from the presetting country list.

Check your ISP immediately for the setting/configuration details.

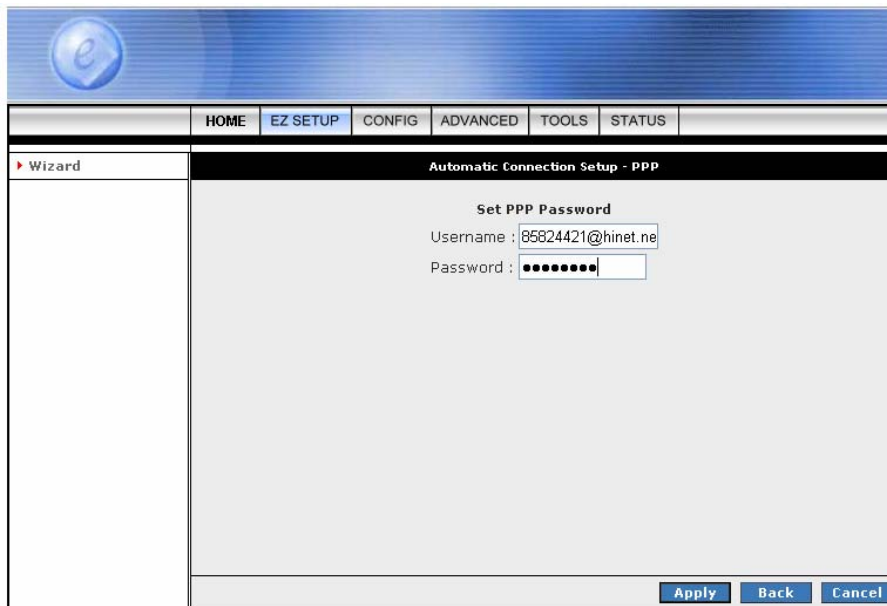
The “**Encapsulation**” type differs in each country and there are two different kinds of setup windows wizard that will pop-up:

A. For the following “**Encapsulation**” type after clicking the “**Next**” button, the pop-up setup window wizard is shown below:

☒ **PPPoA VC-Mux**

☒ **PPPoA LLC**

☒ **PPPoE LLC**



The screenshot shows a web-based configuration interface for a router. At the top, there is a blue header with a logo. Below it is a navigation bar with tabs: HOME, EZ SETUP (selected), CONFIG, ADVANCED, TOOLS, and STATUS. On the left side, there is a sidebar with a 'Wizard' link. The main content area is titled 'Automatic Connection Setup - PPP'. It contains a section 'Set PPP Password' with two input fields: 'Username' (containing '85824421@hinet.ne') and 'Password' (containing masked characters). At the bottom right of the main area, there are three buttons: 'Apply', 'Back', and 'Cancel'.

Manually enter your “**User Name**” and “**Password**” which will be provided by your Service Provider (ISP). Click “**Apply**” after setup.

B. For countries with the following “**Encapsulation**” type after clicking the “**Next**” button, the pop-up window is shown below:

- ☒ **1483 Bridged LLC**
- ☒ **1483 Routed VC-MUX**

The screenshot shows the 'Automatic Setup' window of an ADSL Router configuration wizard. The window has a blue header with a logo and a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. The 'EZ SETUP' tab is active. On the left, there is a 'Wizard' sidebar. The main area is titled 'Automatic Setup' and contains the following fields and options:

- Set Area**
 - Country : Argentina (dropdown)
 - ISP : Argentina Telecom (dropdown)
 - encapsulation : 1483 Bridged LLC (text box)
 - VPI : 0 (text box)
 - VCI : 33 (text box)
- Connection Type :**
 - ☒ **Static (Fixed IP by ISP)**
 - ☐ DHCP (Get IP dynamically from ISP)
 - ☐ Bridge

Below the connection types, there is a note: 'If you can't find your ISP setting, please click **Config** to config yourself.' At the bottom right, there are 'Next' and 'Cancel' buttons.

In this current window, you will find **THREE** different **Connection Type**:

1. **Static (Fixed IP by ISP):** Click the radio button to enable **Static (Fixed IP by ISP)** option, then click “Next”, the following window will pop-up:

The screenshot shows a web-based configuration interface for a router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. The 'EZ SETUP' tab is active, and a 'Wizard' sidebar is on the left. The main content area is titled 'Automatic Connection Setup - Static' and contains a 'Set Static IP' section. This section has input fields for IP Address (192.168.12.53), Mask (255.255.255.0), Default Gateway (192.168.12.1), DNS 1 (168.95.1.1), DNS 2, and DNS 3. At the bottom right of the main area are buttons for 'Apply', 'Back', and 'Cancel'.

- **Set IP Address:** Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

- ☒ **“IP Address”:** This is the static IP Address given by the ISP.
Range for IP Address is $x.x.x.y$, where $0 \leq x \leq 255$ and $1 \leq y \leq 254$.

- ☒ **“Mask”:** This is the subnet mask given by the ISP.
Range for Subnet Mask is $x.x.x.x$, where $0 \leq x \leq 255$.

- ☒ **“Default Gateway”:** This is the Gateway given by the ISP.
Range for Gateway is $x.x.x.y$, where $0 \leq x \leq 255$ and $1 \leq y \leq 254$.

- **“DNS”:** This is the DNS address specify by the user or ISP. Check your ISP for setting detail.

Range for DNS Address is $x.x.x.y$, where $0 \leq x \leq 255$ and $1 \leq y \leq 254$.

- Click **“Apply”** after your setting.

2. **DHCP (Get IP dynamically from ISP):** Click the radio button to enable **DHCP (Get IP dynamically from ISP)**. Click “**Next**” after your choice and the following window will pop-up:

The screenshot shows a web-based configuration interface for a router. At the top, there is a blue header with a logo on the left and a navigation bar with tabs: HOME, EZ SETUP (selected), CONFIG, ADVANCED, TOOLS, and STATUS. Below the navigation bar, on the left, is a sidebar with a 'Wizard' link. The main content area is titled 'Automatic Connection Setup - DHCP Client'. It contains the following text: 'DHCP Client', 'IP Address :', 'Mask :', 'Gateway :', and 'Default Gateway :'. A checkbox is checked next to 'Default Gateway :'. At the bottom right of the main area, there are three buttons: 'Apply', 'Back', and 'Cancel'.

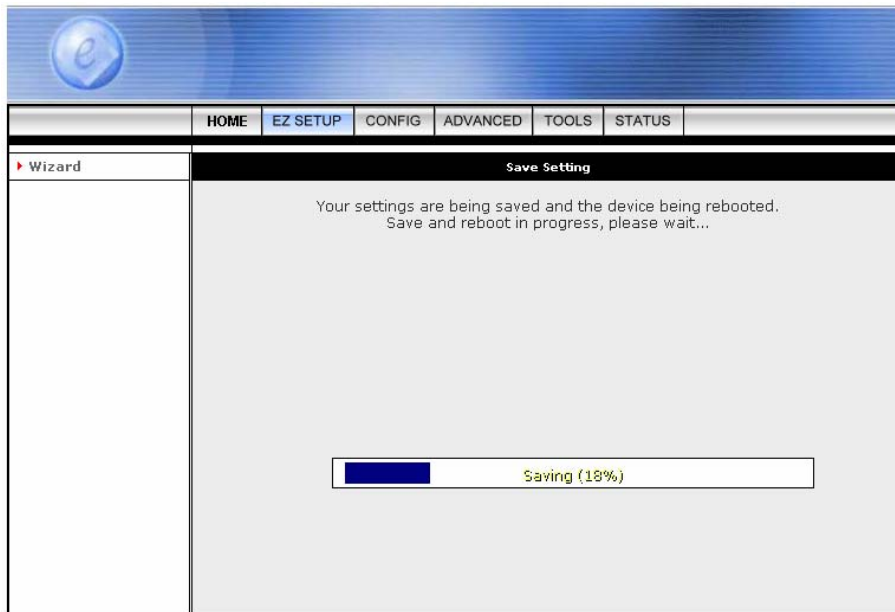
- Place a check to enable the Default Gateway. The Default Gateway Address is provided by the ISP.
- Click “**Apply**” after your setting.

3. **Bridge:** Click the radio button to enable **DHCP (Get IP dynamically from ISP)**. Click **“Next”** after your choice and the following screen will pop-up:

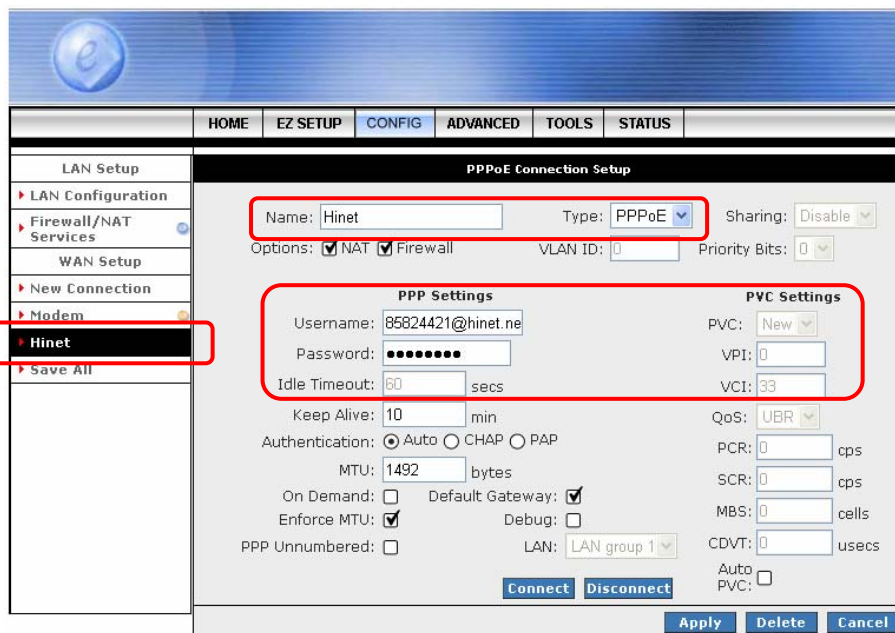
The screenshot shows a web-based configuration interface for a router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. A left sidebar contains a 'Wizard' section with a red arrow. The main content area is titled 'Automatic Connection Setup - Bridge' and features a 'Bridge' section with a 'Select LAN:' label and a dropdown menu currently set to 'LAN group 1'. At the bottom right of the main area are three buttons: 'Apply', 'Back', and 'Cancel'.

- **Select LAN:** Select LAN group from the drop down manual or leave it as it's default then click **“Apply”** after your setting.
- Click **“Apply”** after your setting.

STEP 2. Click “Apply” after setup. Following windows will pop-up.



The device's system will save and activate your setting after clicking the “Apply” button. The following windows will pop up after the reboot process.



- Check the following items when the above window pop-up.
 - ☑ **Name:** Show the ISP name selected in **STEP 1**.
 - ☑ **Type:** Show the **Encapsulation** type selected in **STEP 1**.
 - ☑ **Username:** Show the **Username** manually entered in **STEP 1**.
 - ☑ **Password:** Show the **Password** manually entered in **STEP 1**.
 - ☑ **VPI:** Show the **VPI** setting as shown in **STEP 1**.
 - ☑ **VCI:** Show the **VCI** setting as shown in **STEP 1**.
- A **Connection Profile** (Normally show the ISP Name) will be added to the left side of the configuration frame under **WAN Setup**.

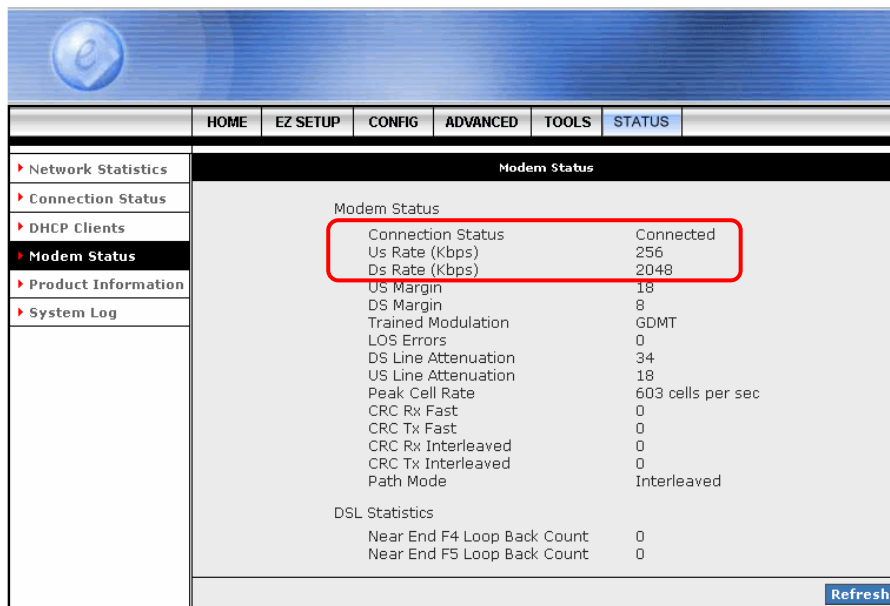
NOTE: If the final setting are differ from what you'd selected in **STEP 1**, click **EZ SETUP** and redo the setup procedures or else check your dealer immediately for technical support.

NOTE: The 4 Ports ADSL2/2+ Router can be configured to maintain up to 8 Connection Profiles. Different Connection Profiles may be required if you connect to more than one ADSL service provider, or if you vary the connection type/setting you use.

Note that in many cases, only one Connection Profile will be required and only one Connection Profile in used at one time.

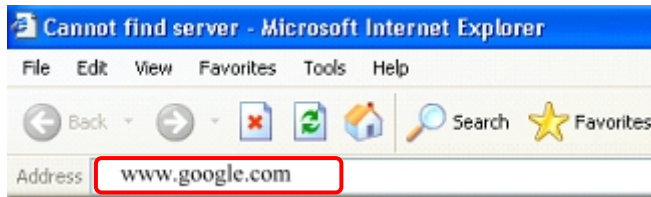
To complete and save the new Connection Profile, click the **Apply** button, and then click **Save All**.

STEP 3. Go to “STATUS” → “Modem Status” and the following window will pop-up. Check the “Connection Status”, “Us Rate” and “Ds Rate”, the numbers/data show you the actual ADSL connection speed in Kbps.

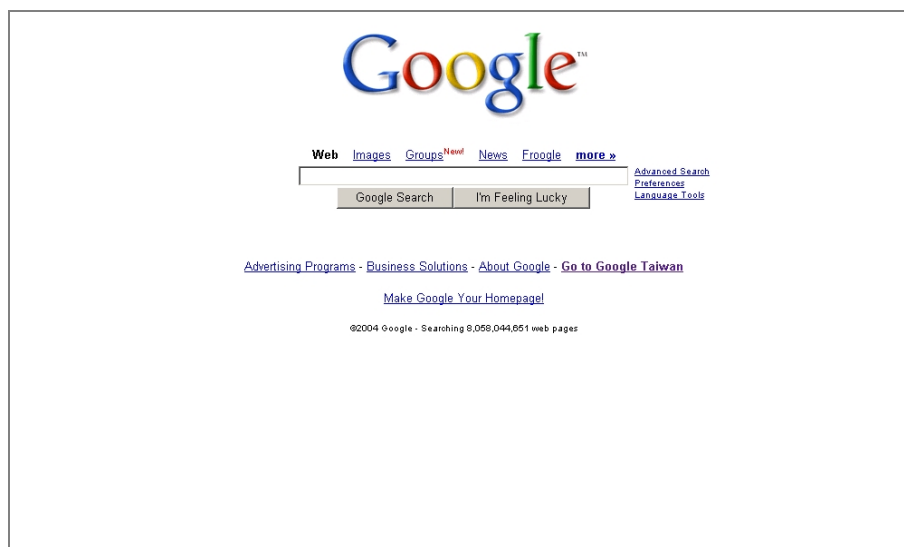


HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS
Modem Status					
Modem Status					
Connection Status Connected					
Us Rate (Kbps) 256					
Ds Rate (Kbps) 2048					
US Margin 18					
DS Margin 8					
Trained Modulation GDMT					
LOS Errors 0					
DS Line Attenuation 34					
US Line Attenuation 18					
Peak Cell Rate 603 cells per sec					
CRC Rx Fast 0					
CRC Tx Fast 0					
CRC Rx Interleaved 0					
CRC Tx Interleaved 0					
Path Mode Interleaved					
DSL Statistics					
Near End F4 Loop Back Count 0					
Near End F5 Loop Back Count 0					
Refresh					

STEP 4. Launch your web browser, and enter the Google Website Address: “**www.google.com**” in the address field then press “**Enter**”.



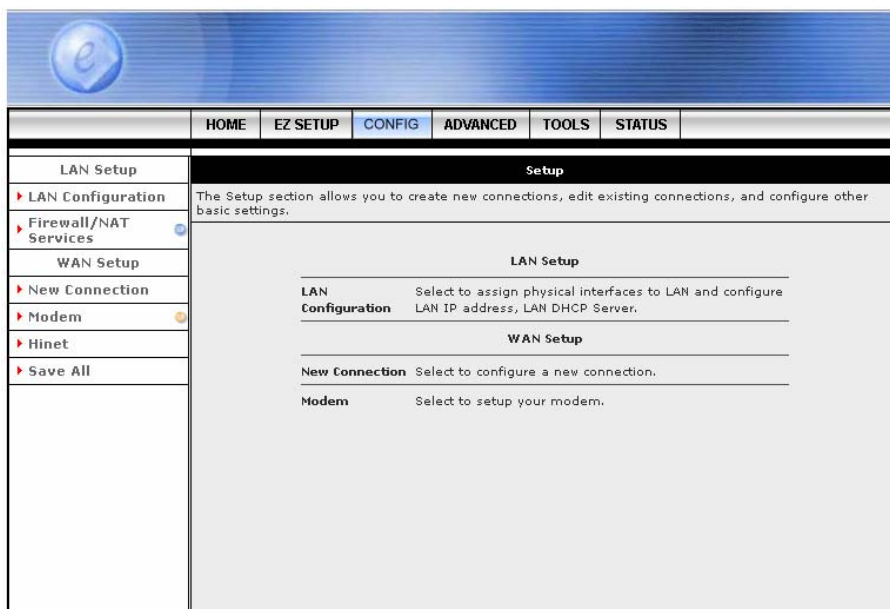
The following Google website index page will display on your screen. This shows your ADSL connection is correctly set and access to the Internet is now available.



4.3 CONFIG

The **CONFIG** configuration page allows you to create new connections, edit existing connections, and configure other basic settings in WAN and LAN mode.

The **CONFIG** Menu is divided into two sections: **LAN Setup** and **WAN Setup**. **WAN Setup** will be dealt with first.



4.3.1 CONFIG - WAN Setup

WAN Setup: The **WAN** configuration page allows you to set the configuration for the WAN/ADSL ports. ADSL connections can be configured in a variety of ways depending on the ISP/WAN configuration, and the requirements of your home or office LAN. This 4 Ports ADSL2/2+ Router supports the following ADSL connection types:

- ☒ PPPoE (RFC2516)
- ☒ PPPoA (RFC2364)
- ☒ DHCP
- ☒ Static
- ☒ Bridged (RFC1483)
- ☒ CLIP (RFC1577)

Configuring the 4 Ports ADSL2/2+ Router to match these connection types may require entry of some or all of the following values:

- ☒ ISP Account Username and Password
- ☒ VPI/VC1 Setting
- ☒ Encapsulation Type/Multiplexing (Either LLC or VC, check with your ISP for details)
- ☒ ADSL Handshaking Mode (Default setting is MMODE)
- ☒ Network Settings for Bridged Mode operation:

For Bridged Mode connections (RFC1483), the ISP will need to provide the following information:

- ☒ DSL Fixed Internet IP address
- ☒ Subnet Mask
- ☒ Default Gateway IP Address
- ☒ Primary DNS IP address.

The next sections will describe in detail how to set up each of these connection types and save them as Connection Profiles.

4.3.1.1 CONFIG - WAN Setup – New Connection

Click **New Connection** to setup a new connection profile. Different connection profiles may be required if you connect to more than one ADSL service provider, or if you vary the connection type you use, or if this 4 Ports ADSL2/2+ Router is used in different locations or countries.

This 4 Ports ADSL2/2+ Router can be configured to maintain up to 8 Connection Profiles.

The **WAN Setup** configuration page enable the user to create, save and select connection profiles as required. (In many cases, only one connection profile will be required and only one connection profile will be used at one time).

To complete and save the new Connection Profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.1 New Connection - PPPoE Connection Setup

PPPoE: When **PPPoE Mode** is selected, the following screen will pop-up. Point-to-Point Protocol (PPP) is a method of establishing a network connection between network hosts. PPPoE, also known as RFC 2516, adapts PPP to work over Ethernet for ADSL connections. PPPoE provides a mechanism for authenticating users by providing User Name and Password fields and it is a connection type provided by many ISP or Telecom.

- **Name:** Enter the PPPoE connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : PPPoE.
- **Sharing:** Select “Disable”, “Enable” or “VLAN” sharing. Default setting is “Disable”.
- **Options:** Click to enable “NAT” and/or “Firewall” functionality. Default is “Enable”.
- **VLAN ID:** If “VLAN” is selected, manually enter the “VLAN ID” and select “Priority Bits” from the drop down manual.
- **PPP Settings:**
 - ☑ **Username:** Your ISP Account ID. Check your ISP for details.
 - ☑ **Password:** Your ISP Account Password. Check your ISP for details.
 - ☑ **Idle Timeout:** The Idle Timeout allows you to set the specific period of time, in seconds, to disconnect from the ISP if the link has no activity detected.
 - ☑ **Keep Alive:** When the On-Demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter 0 in this field.

- ☒ **Authentication:** The different types of available authentications are:
 - **Auto:** When auto is selected, PAP mode will run by default. However, if PAP fails, then will run as the secondary protocol. This is the default setting.
 - **PAP:** Password Authentication Procedure. Authentication is done through username and password.
 - **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.
- ☒ **MTU:** Maximum Transmission Unit. The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. This can be set from a minimum 128 to maximum 1500.
- ☒ **On Demand:** If enable On Demand mode, the connection will be dropped if no activity is detected after the specified Idle Timeout value.
- ☒ **Default Gateway:** Check box to make this the default connection.
- ☒ **Enforce MTU:** Check box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to PPP MTU. MTU (Maximum Transmission Unit) is defined as the maximum packet size (In bytes), that a particular interface can handle.
- ☒ **Debug:** Click to enable the PPP connection debugging facilities.
- ☒ **PPP Unnumbered:** Click to enable PPP Unnumbered function then select LAN Group from the LAN dropdown manual.
- **PVC Settings:**
 - ☒ **PVC:** This field allows you to choose the specific PVC for the PPP session.
 - ☒ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
 - ☒ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
 - ☒ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
 - ☒ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
 - ☒ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
 - ☒ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.

- ☒ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☒ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.
- **Connect:** Click **Connect** to establish a PPP connection under this connection profile.
- **Disconnect:** Click **Disconnect** to drop the PPP connection under this connection profile.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.1.2 New Connection - PPPoA Connection Setup

PPPoA: When **PPPoA** mode is selected, the following screen will pop-up. Point-to-Point Protocol (PPP) is a method of establishing a network connection between network hosts. PPPoA, also known as RFC 2346, adapts PPP to work over ATM cells for ADSL connections.

- **Name:** Enter the PPPoA connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : PPPoA.
- **Options:** Click to enable “NAT” and/or “Firewall” functionality. Default is “Enable”.
- **PPP Settings:**
 - ☑ **Username:** Your ISP Account ID. Check your ISP for details.
 - ☑ **Password:** Your ISP Account Password. Check your ISP for details.
 - ☑ **Idle Timeout:** The Idle Timeout allows you to set the specific period of time, in seconds, to disconnect from the ISP if the link has no activity detected.
 - ☑ **Keep Alive:** When the On-Demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter 0 in this field.
 - ☑ **Authentication:** The different types of available authentications are:
 - **Auto:** When auto is selected, PAP mode will run by default. However, if PAP fails, then will run as the secondary protocol. This is the default setting.
 - **PAP:** Password Authentication Procedure. Authentication is done through username and password.
 - **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

- ☒ **MTU:** Maximum Transmission Unit. The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. This can be set from a minimum 128 to maximum 1500.
- ☒ **On Demand:** If enable On Demand mode, the connection will be dropped if no activity is detected after the specified Idle Timeout value.
- ☒ **Default Gateway:** Check box to make this the default connection.
- ☒ **Debug:** Click to enable the Debug function. The complete debugging information will show and listed in the System Log file.
- ☒ **PPP Unnumbered:** Click to enable PPP Unnumbered function then select LAN Group from the LAN dropdown manual.
- **PVC Settings:**
 - ☒ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
 - ☒ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
 - ☒ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
 - ☒ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
 - ☒ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
 - ☒ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
 - ☒ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
 - ☒ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.
- **Connect:** Click **Connect** to establish a PPP connection under this connection profile.
- **Disconnect:** Click **Disconnect** to drop the PPP connection under this connection profile.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.1.3 New Connection - Static Connection Setup

Static: When Static mode is selected, the following screen will pop-up. Most Internet users are provided with a dynamic IP address by their ISP for each session, however certain situations call for a Static IP address. This is typically when you want to host a website, or use VoIP or video-conferencing applications where other users must regularly connect to your computer. Static IP numbers are generally made available by ISPs for these purposes for an additional fee.

The screenshot shows the 'Static Connection Setup' window. The sidebar on the left includes 'LAN Setup', 'LAN Configuration', 'Firewall/NAT Services', 'WAN Setup', 'New Connection' (highlighted), 'Modem', 'Hinet', and 'Save All'. The main configuration area is titled 'Static Connection Setup' and includes the following fields and options:

- Name:** Static
- Type:** Static (dropdown)
- Sharing:** Disable (dropdown)
- Options:** ☒ NAT, ☒ Firewall
- VLAN ID:** 0
- Priority Bits:** 0 (dropdown)
- Static Settings:**
 - Encapsulation:** ☒ LLC, ☐ VC
 - IP Address:** 192.168.12.53
 - Mask:** 255.255.255.255
 - Default Gateway:** 192.168.12.1
 - DNS 1:** 192.68.1.1
 - DNS 2:** (empty)
 - DNS 3:** (empty)
 - Mode:** ☒ Bridged, ☐ Routed
- PVC Settings:**
 - PVC:** New (dropdown)
 - VPI:** 0
 - VCI:** 33
 - QoS:** UBR (dropdown)
 - PCR:** 0 cps
 - SCR:** 0 cps
 - MBS:** 0 cells
 - CDVT:** 0 usecs
 - Auto PVC:** ☐

Buttons at the bottom right: Apply, Delete, Cancel.

- **Name:** Enter the Static connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : Static.
- **Sharing:** Select “Disable”, “Enable” or “VLAN” sharing. Default setting is “Disable”.
- **Options:** Click to enable “NAT” and/or “Firewall” functionality. Default is “Enable”.
- **VLAN ID:** If “VLAN” is selected, manually enter the “VLAN ID” and select “Priority Bits” from the drop down manual.
- **Static Settings:**
 - ☒ **Encapsulation:** Select the encapsulation type (LLC or VC) according to the information provided by the ISP.
 - ☒ **IP Address:** Enter the IP Address provided by your ISP.
 - ☒ **Mask:** Enter the Subnet mask specified by your ISP.
 - ☒ **Default Gateway:** Enter the Default Gateway as specified by the ISP.
 - ☒ **DNS:** Up to three Domain Name Server (DNS) addresses can also be specified.
 - ☒ **Mode:** For static configuration, you can also select a bridge connection or a routed connection. Since a Static IP address is typically used to host WEB servers, Bridged connection is usual however Routed is provided also. Check with ISP for confirmation.

■ **PVC Settings:**

- ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
- ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
- ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
- ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
- ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
- ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.

■ **Apply:** Click **Apply** to complete and save the connection profile.

■ **Delete:** Click **Delete** to delete a connection.

■ **Cancel:** Click **Cancel** to ignore all the changes.

■ **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.1.4 New Connection - DHCP Connection Setup

DHCP: When DHCP mode is selected, the following screen will pop-up. Dynamic Host Configuration Protocol (DHCP) allows the ADSL Router to automatically obtain the IP address from the server. This option is commonly used in situations where the IP address is dynamically assigned and is not known prior to assignment.

The screenshot shows a web-based configuration interface for an ADSL router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG (selected), ADVANCED, TOOLS, and STATUS. On the left, a sidebar menu lists various setup options: LAN Setup, LAN Configuration, Firewall/NAT Services, WAN Setup, New Connection (highlighted), Modem, Hinet, and Save All. The main content area is titled 'DHCP Connection Setup'. It contains several fields and sections: 'Name' (set to 'DHCP'), 'Type' (set to 'DHCP'), and 'Sharing' (set to 'Disable'). Below these are 'Options' for NAT and Firewall (both checked), 'VLAN ID' (set to 0), and 'Priority Bits' (set to 0). The 'DHCP Settings' section includes 'Encapsulation' (radio buttons for LLC and VC, with LLC selected), 'IP Address', 'Mask', 'Gateway', and 'Default Gateway' (checked). There are 'Renew' and 'Release' buttons. The 'PVC Settings' section includes a 'PVC' dropdown (set to 'New'), 'VPI' (0), 'VCI' (33), 'QoS' (UBR), and several rate limiters: PCR (0 cps), SCR (0 cps), MBS (0 cells), and CDVT (0 usecs). An 'Auto PVC' checkbox is at the bottom. At the very bottom of the form are 'Apply', 'Delete', and 'Cancel' buttons.

- **Name:** Enter the DHCP connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : DHCP.
- **Sharing:** Select “Disable”, “Enable” or “VLAN” sharing. Default setting is “Disable”.
- **Options:** Click to enable “NAT” and/or “Firewall” functionality. Default is “Enable”.
- **VLAN ID:** If “VLAN” is selected, manually enter the “VLAN ID” and select “Priority Bits” from the drop down manual.
- **DHCP Settings:**
 - ☑ **Encapsulation:** Select the encapsulation type (LLC or VC) according to the information provided by the ISP.
 - ☑ **Default Gateway:** Click to enable the Default Gateway.
- **PVC Settings:**
 - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
 - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
 - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.

- ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
- ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
- ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.
- **Renew:** Click the **Renew** button and the gateway will retrieve the IP Address, Subnet Mask, and Gateway Address.
- **Release:** Click the **Release** button to release the IP Address, Subnet Mask and Gateway Address.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.1.5 New Connection - Bridge Connection Setup

Bridge: When Bridge mode is selected, the following screen will pop-up. A Bridged connection basically disables the routing, firewall and NAT features of the 4 Ports ADSL2/2+ Router. In a Bridged connection, the 4 Ports ADSL2/2+ Router acts as a modem or hub, and just transmits packets between the WAN interface and the LAN interface. A Bridged connection assumes that another device is providing the routing functionality that is now disabled in the 4 Ports ADSL2/2+ Router.

The screenshot shows the 'Bridged Connection Setup' window. The sidebar on the left has a tree view with the following items: LAN Setup, LAN Configuration, Firewall/NAT Services, WAN Setup, New Connection, Modem, Hinet, and Save All. The main content area is titled 'Bridged Connection Setup' and contains the following fields and sections:

- Name:** Bridge
- Type:** Bridge
- Sharing:** Disable
- Options:**
- VLAN ID:** 0
- Priority Bits:** 0
- Bridge Settings:**
 - Encapsulation:** LLC (selected), VC
 - Select LAN:** LAN group 1
- PVC Settings:**
 - PVC:** New
 - VPI:** 0
 - VCI:** 33
 - QoS:** UBR
 - PCR:** 0 cps
 - SCR:** 0 cps
 - MBS:** 0 cells
 - CDVT:** 0 usecs
 - Auto PVC:** (unchecked)

At the bottom of the window are three buttons: Apply, Delete, and Cancel.

- **Name:** Enter the Bridge connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : DHCP.
- **Sharing:** Select “Disable”, “Enable” or “VLAN” sharing. Default setting is “Disable”.
- **VLAN ID:** If “VLAN” is selected, manually enter the “VLAN ID” and select “Priority Bits” from the drop down manual.
- **Bridge Settings:**
 - ☑ **Encapsulation:** Select the encapsulation type (LLC or VC) according to the information provided by the ISP.
 - ☑ **Select LAN:** Up to three LAN Group can be specified. Select your LAN Group from the drop down manual.
- **PVC Settings:**
 - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
 - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
 - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.

- ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
- ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
- ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.1.6 New Connection - CLIP Connection Setup

CLIP: When CLIP mode is selected, the following screen will pop-up. The Classical IP over ATM (CLIP) support provides the ability to transmit IP packets over an ATM network, CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577 and utilizes an ATM-aware version of the ARP protocol.

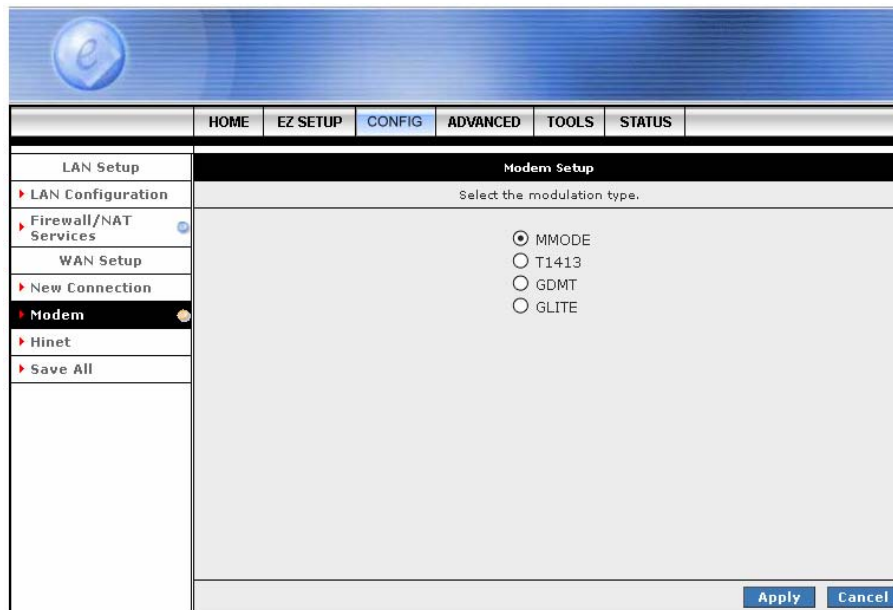
The screenshot shows the 'CLIP Connection Setup' window. The sidebar on the left includes 'LAN Setup', 'LAN Configuration', 'Firewall/NAT Services', 'WAN Setup', 'New Connection' (highlighted), 'Modem', 'Hinet', and 'Save All'. The main panel has tabs: HOME, EZ SETUP, CONFIG (selected), ADVANCED, TOOLS, and STATUS. The 'CLIP Connection Setup' section includes:
- Name: CLIP
- Type: CLIP (dropdown)
- Sharing: Disable (dropdown)
- Options: ☒ NAT, ☒ Firewall
- VLAN ID: 0
- Priority Bits: 0 (dropdown)
- CLIP Settings:
 - IP Address: 192.168.12.12
 - Mask: 255.255.255.0
 - ARP Server: 0.0.0.0
 - Default Gateway: (empty)
- PVC Settings:
 - PVC: New (dropdown)
 - VPI: 0
 - VCI: 33
 - QoS: UBR (dropdown)
 - PCR: 0 cps
 - SCR: 0 cps
 - MBS: 0 cells
 - CDVT: 0 usecs
 - Auto PVC: ☐
Buttons at the bottom right: Apply, Delete, Cancel.

- **Name:** Enter the CLIP connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : CLIP.
- **CLIP Settings:**
 - ☒ **IP Address:** Enter the IP Address provided by your ISP.
 - ☒ **Mask:** Enter the Subnet mask specified by your ISP.
 - ☒ **ARP Server:** Leave as Default (0.0.0.0) unless advised by ISP.
 - ☒ **Default Gateway:** Enter the Default Gateway as specified by the ISP.
- **PVC Settings:**
 - ☒ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
 - ☒ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
 - ☒ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
 - ☒ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.

- ☒ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☒ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☒ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☒ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports ADSL2/2+ Router.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.1.2 CONFIG - WAN Setup - Modem

Modem: This field allows you to select from the following ADSL handshake protocols. Check your ISP for the connection type.



The screenshot shows a web-based configuration interface for a router. At the top, there is a navigation bar with tabs: HOME, EZ SETUP, CONFIG (selected), ADVANCED, TOOLS, and STATUS. Below the navigation bar is a sidebar menu with options: LAN Setup, LAN Configuration, Firewall/NAT Services, WAN Setup, New Connection, Modem (selected), Hinet, and Save All. The main content area is titled 'Modem Setup' and contains the instruction 'Select the modulation type.' Below this instruction are four radio button options: MMODE (selected), T1413, GDMT, and GLITE. At the bottom right of the main content area are two buttons: 'Apply' and 'Cancel'.

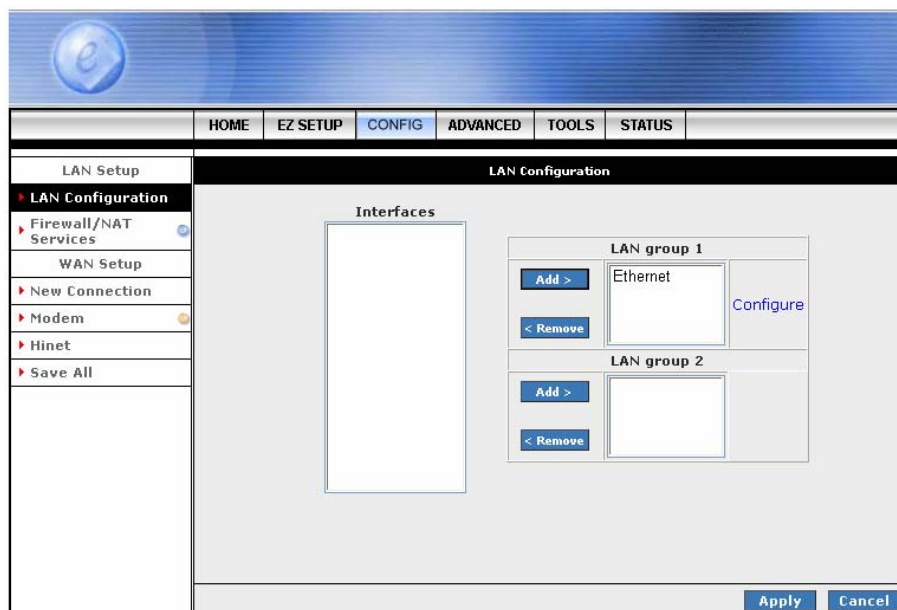
- **MMODE:** Multiple Mode (Default).
- **T1413:** T1.413 Mode.
- **GDMT:** G.dmt Mode.
- **GLITE:** G.Lite Mode.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2 CONFIG - LAN Setup

The **LAN Configuration** pages allow you to select or assign physical interfaces to LAN group and configure LAN IP Address and DHCP functionality.

4.3.2.1 LAN Setup - LAN Configuration

Click LAN Configuration and the following screen will be shown.



- Click **Add** or **Remove** Interfaces from list under the different LAN Group. The LAN Group features only supported under **Bridge Mode** setting. Interfaces under the same LAN Group (Ethernet and USB(Optional)) will have the ability to communicate with each other. Different LAN Group are prohibited to communicate with one another.
- Click **Configure** for detail LAN Group setting. Refer to next section for detail configuration and setting.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.1 LAN Configuration - Unmanaged

Unmanaged: Click the **Unmanaged** radio button, the following configuration screen will pop-up. All filling items are hidden except the **Server and Relay Off** (Unchangeable) radio button will turn on.

Click the **Services** items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.

The screenshot shows the 'LAN Group 1 Configuration' window. The sidebar on the left has a tree view with the following items: LAN Setup, LAN Configuration (selected), Firewall/NAT Services, WAN Setup, New Connection, Modem, Hinet, and Save All. The main content area is titled 'LAN Group 1 Configuration' and contains the following sections:

- IP Settings:**
 - ☒ Unmanaged
 - ☐ Obtain an IP address automatically
 - IP Address: [Release](#)
 - Netmask: [Renew](#)
 - ☐ PPP IP Address
 - IP Address:
 - ☐ Use the following Static IP address
 - IP Address:
 - Netmask:
 - Default Gateway:
 - Host Name:
 - Domain:
 - ☐ Enable DHCP Server
 - Start IP:
 - End IP:
 - Lease Time: Seconds
 - ☐ Enable DHCP Relay
 - Relay IP:
 - ☒ Server and Relay Off
- Services:**
 - IP Filters ☒
 - Bridge Filters ☐
 - UPnP ☐
 - LAN Clients ☒
 - IP QoS ☐
 - Static Routing ☐

At the bottom right of the window are [Apply](#) and [Cancel](#) buttons.

- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.2 LAN Configuration – Obtain an IP Address Automatically

Obtain an IP address automatically: The following configuration screen will pop-up. All filling items will be hidden except **Host Name**, **Domain Name** and **Server and Relay Off** (Unchangeable) radio button will turn on.

Click **Services** selection items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.

Services	Status
IP Filters	
Bridge Filters	
UPnP	
LAN Clients	
IP QoS	
Static Routing	

- **Host Name:** Can be any alpha-numeric expression that does not contain spaces.
- **Domain Name:** Used in conjunction with the host name to uniquely identify the gateway. To access the 4 Ports ADSL2/2+ Router's web pages, the user can type **192.168.1.1** (The default IP Address) or type **mygateway1.ar7** in the Web browser's address bar.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.3 LAN Configuration – PPP IP Address

PPP IP Address: The following configuration screen will pop-up. All filling items will be hidden except the **Server and Relay Off** (Unchangeable) radio button will turn on.

Click **Services** selection items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.

The screenshot displays the 'LAN Group 1 Configuration' window. On the left is a sidebar with a tree view containing 'LAN Setup', 'LAN Configuration' (selected), 'Firewall/NAT Services', 'WAN Setup', 'New Connection', 'Modem', 'Hinet', and 'Save All'. The main area is titled 'LAN Group 1 Configuration' and contains 'IP Settings' and 'Services' sections. In 'IP Settings', the 'PPP IP Address' radio button is selected, with the IP address field set to '192.168.1.1'. Other options include 'Unmanaged', 'Obtain an IP address automatically', and 'Use the following Static IP address'. The 'Services' section on the right lists 'IP Filters', 'Bridge Filters', 'UPnP', 'LAN Clients', 'IP QoS', and 'Static Routing', each with a status indicator. At the bottom are 'Apply' and 'Cancel' buttons.

- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.4 LAN Configuration – Use The Following Static IP Address

Use the following **Static IP address**: The following configuration screen will pop-up.

Click the radio button to select **Enable DHCP Server** or **Enable DHCP Relay** or **Server and Relay Off**. Manually enter the necessary items based on each selection.

- **IP Address:** This is the static IP Address given by the ISP.
- **Netmask:** This is the subnet mask given by the ISP.
- **Default Gateway:** This is the Gateway given by the ISP.
- **Host Name:** Can be any alpha-numeric expression that does not contain spaces.
- **Domain:** Used in conjunction with the host name to uniquely identify the gateway.
- **Enable DHCP Server:** Click the radio button to enable the DHCP Server.
 - ☑ **Start IP:** The Start IP Address indicates the beginning of the range at which the DHCP server starts issuing IP addresses.

This value must be greater than the Routers IP address value. If the Routers IP address is 192.168.1.1 (The default) than the starting IP address must be 192.168.1. 2 or higher.
 - ☑ **End IP:** The End IP Address indicates the end of the IP address range.

The ending address must not exceed a Subnet Limit of 253; hence the maximum value that can be entered in this example is 192.168.1.254.
 - ☑ **Lease Time:** Lease Time is the amount of time a network user will be allowed connection to the 4 Ports ADSL2/2+ Router with their current Dynamic IP address. The amount of time is in units of minutes; the default value is 3600 minutes (60 hours).

- **Enable DHCP Relay:** Click the radio button to enable the DHCP Relay.
 - ☒ **Relay IP:** This is the IP Address given by the ISP.

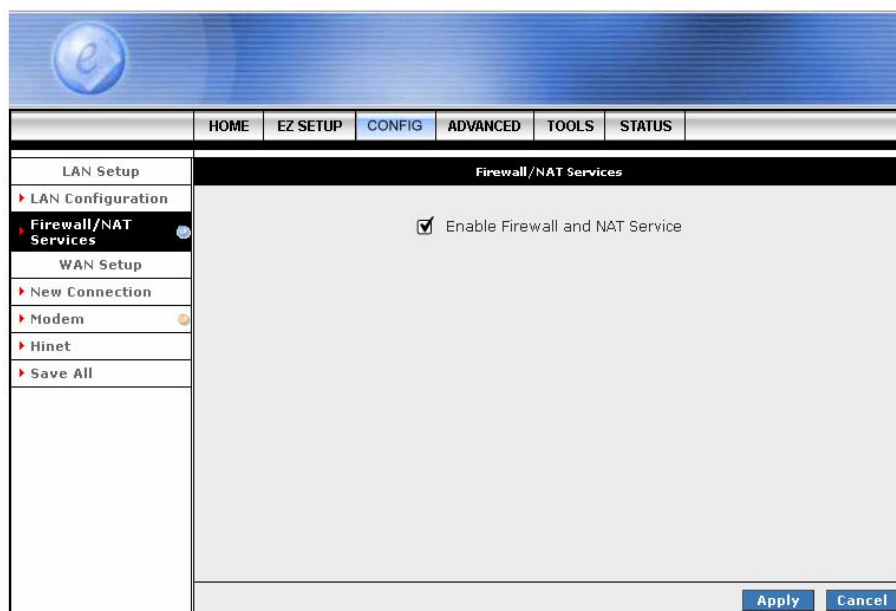
- **Server and Relay Off:** Click the radio button to enable.

Caution: If the **Server and Relay Off** function is selected, careful attention must be paid to the IP Address setup of each computer on the LAN. IP Addresses will no longer be allocated automatically.

- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.3 LAN Setup - Firewall/NAT Services

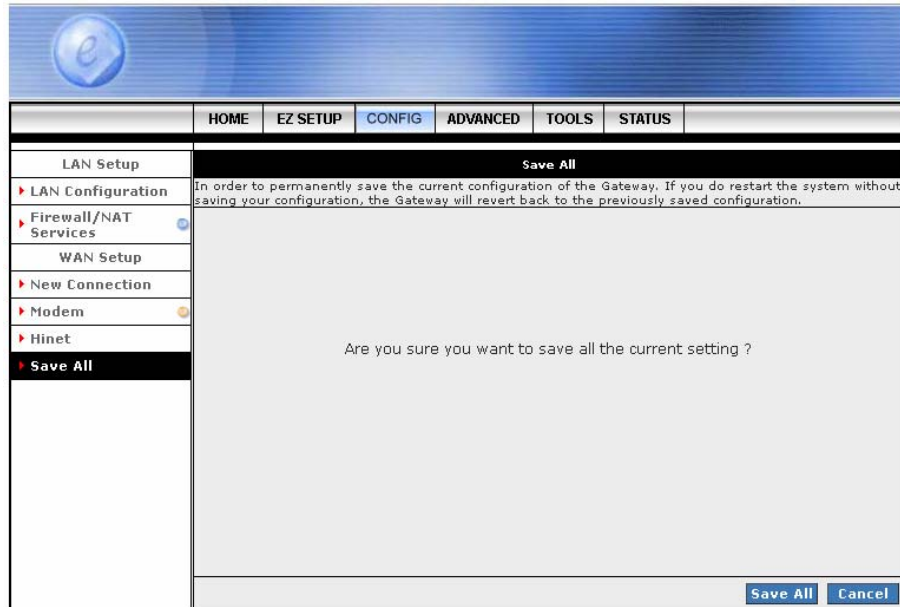
Firewall/NAT Services: Place a check to “**Enable**” the most basic Firewall and NAT Service to secure your system. The 4 Ports ADSL2/2+ Router is equipped with advanced Firewall features to provide security from malicious attack, hacking or eavesdropping across the Internet. It’s strongly recommend that you enable this feature for security purpose. The default setting is “**Enable**”.



- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.4 CONFIG – Save All

Save All: Click **Save All** in order to permanently save the current configuration of the 4 Ports ADSL2/2+ Router. If you do restart the system without saving your configuration, the 4 Ports ADSL2/2+ Router will revert back to the previously saved configuration.



- **Save All:** Click **Save All** to complete and permanently save the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.

4.4 ADVANCED

The Advanced Menu provides access to advanced networking, management and routing capabilities. Click the **ADVANCED** tab and the following screen will pop-up.

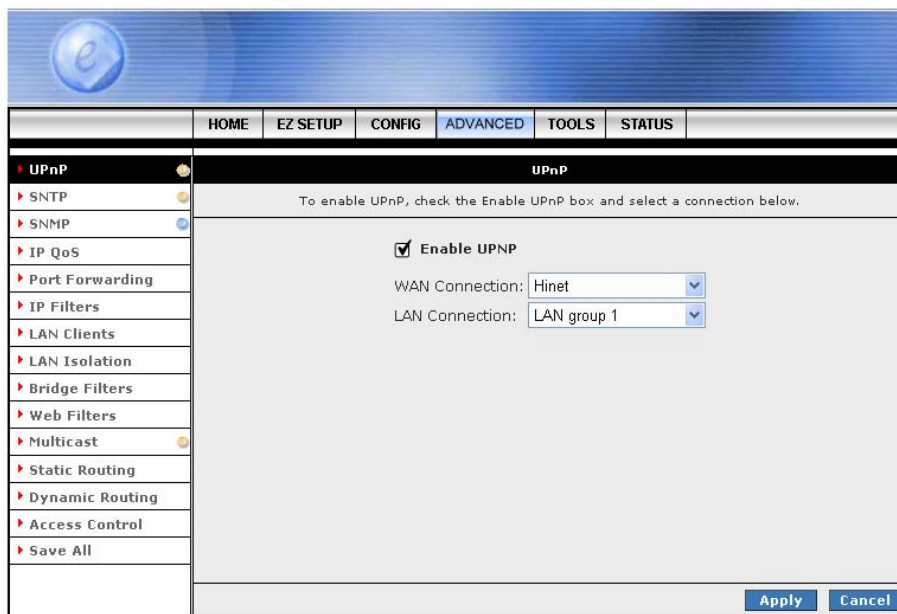


- **UPnP:** Configure UPnP for different connections.
- **SNTP:** Configure SNTP to configure time server on Internet.
- **SNMP:** Configure SNMP Management.
- **IP QoS:** Configure IP Quality of Service for different connections.
- **Port Forwarding:** Configure Firewall and NAT pass-through to your hosted applications.
- **IP Filters:** Configure Firewall to block your LAN PCs from accessing the Internet.
- **LAN Clients:** Configure LAN Clients.
- **LAN Isolation:** Disable traffic between LANs.
- **Bridge Filters:** Select to setup Bridge Filters.
- **Web Filters:** Select to setup Web Filters.
- **Multicast:** Configure Multicast pass-through for different connections.
- **Static Routing:** Configure Static routes.
- **Dynamic Routing:** Configure RIP.
- **Access Control:** Configure access control list.
- **Save All:** Click in order to permanently save the current configuration.

4.4.1 ADVANCED - UPnP

UPnP: Universal Plug and Play is a protocol which automates connectivity between network devices, including computers, game consoles, digital cameras and other systems which connect via TCP/IP. Applications which implement the UPnP protocol are able to negotiate a connection with a UPnP-enabled device without requiring manual device configuration.

To enable UPnP, place a check at the **Enable UPNP**. This will reveal the Enable UPnP screen. UPnP can only be enabled on a saved Connection Profile (Refer to **EZ SETUP** or **CONFIG → WAN Setup** for information on creating Connection Profiles).



- **Enable UPNP:** Place a check to enable the UPnP feature.
- **WAN Connection:** Select the required **WAN Connection Profile** by clicking on the drop down button adjacent to the Connection Profile name.
- **LAN Connection:** Select the **LAN Group** from the drop down manual.
- **Apply:** Click **Apply** to complete and save the connection profile.
- **Cancel:** Click **Cancel** to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.2 ADVANCED - SNTP

SNTP: Simple Network Time Protocol is an efficient method of obtaining the time from a Time Server. Place a check at Enable SNTP to enable the SNTP functionality.

The screenshot shows the configuration interface for the 4 Ports ADSL2/2+ Router. The 'ADVANCED' tab is selected in the top navigation bar. On the left, a sidebar lists various configuration options, with 'SNTP' highlighted. The main content area is titled 'SNTP' and contains the following settings:

- ☒ **Enable SNTP**
- Primary SNTP Server:
- Secondary SNTP Server:
- Tertiary SNTP Server:
- Timeout: Secs
- Polling Interval: Mins
- Retry Count:
- Time Zone:
- Day Light: ☐

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

- **Enable SNTP:** Place a check to enable SNTP feature.
- **SNTP Server:** Enter the SNTP Server IP Address. This 4 Ports ADSL2/2+ Router support up to three SNTP Server IP Address; **Primary**, **Secondary** and **Tertiary SNTP Server**.
- **Timeout:** A time limit for an operation.
- **Polling Interval:** The length of time (In Minutes) the 4 Ports ADSL2/2+ Router retrieves the time from the SNTP Server.
- **Retry Count:** Enter the Retry Count to access the SNTP Server.
- **Time Zone:** This specifies the time zone (Geographical location).
- **Day Light:** Place a check at the Day Light to activate Daylight Savings Time.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.3 ADVANCED - SNMP

SNMP: Simple Network Management Protocol (SNMP) is an application layer protocol that is used for managing networks. There are several components that make up the SNMP structure, including agents, network management stations (NMS), network management protocols, and a management information base (MIB).

The screenshot shows a web-based configuration interface for a router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left, a sidebar menu lists various configuration options: UPnP, SNTP, SNMP (selected), IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area is titled 'SNMP Management' and contains the following settings:

- ☒ Enable SNMP Agent
- ☒ Enable SNMP Traps
- Name:
- Location:
- Contact:
- Community**

Name	Access Right
Public	ReadOnly
Non-Public	ReadWrite
- Traps**

Destination IP	Trap Community	Trap Version
10.0.0.3		SNMP v1
		SNMP v2c

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

- **SNMP Agent:** Click to enable the **SNMP Agent**. An SNMP agent is a node that resides on the network, typically a computer or a router. The SNMP agent is controlled and configured by the NMS by sending SNMP messages between one another. SNMP agents are logged and identified in a Management Information Base (MIB), in which they are identified by an object identifier (OID).
- **SNMP Traps:** Click to enable the **SNMP Traps**. SNMP traps are used to notify network managers of significant events that have taken place in the network. These traps are sent to the SNMP NMS (NMS Server located at Trap IP) through the specified Ports.
- **SNMP System Identification:** The **Name**, **Contact**, **Location** and **Vendor OID** (Optional) are provided to identify the SNMP NMS. The Vendor OID is the ID number placed in all Trap reports. *The System Name, System Contact, and System Location can be up to 127 characters.*
- **Community ReadOnly:** This is the password to access public information. The Community ReadOnly can be up to 127 characters. Default is “**Public**”.
- **Community ReadWrite:** This is the password to access private information. The Community ReadWrite can be up to 127 characters.

- **Trap Destination IP:** This is the IP address to which SNMP traps are sent. There can be up to 5 different SNMP trap destination IP addresses.
- **Trap Community:** This is the password to access and view SNMP traps. The Trap Community can be up to 127 characters. Default is “**Trap community**”.
- **Trap Version:** Select from Version 1 or Version v2c. Default is “**Version 1**”.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.4 ADVANCED - IP QoS

IP QoS: IP Quality of Service (QoS) prioritize data streams to ensure that basic connectivity is maintained when running multiple services over one connection.

For example, if you are using a peer-to-peer file-sharing program at the same time as performing normal web browsing, you can configure QoS to limit the resources dedicated to the peer-to-peer session in order to ensure web browser connectivity.

Leave it at its default setting if you do not know the QoS.

IP QoS											
Choose a connection: Hinet											
Low priority weight: 40%											
Medium priority weight: 60%											
Enable IPQoS: ☒											
Trusted Mode: ☐											
Name	Source IP	Source Port	Start	Destination IP	Destination Port	Start	Protocol	Priority	Phy Port	TOS	Delete

Add

Apply Cancel

- **Choose a connection:** Click to select a LAN group from the drop down manual.
- **Low priority weight :** Click to select the low priority weight from the drop down manual. The default is 40%.
- **Medium priority weight:** Click to select the low priority weight from the drop down manual. The default is 60%.
- **Enable IPQoS:** Click to enable IP QoS features.
- **Trusted Mode:** Click to enable Trusted Mode.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.

- **Add:** To add an IP QoS session, place a check at the Enable IPQoS then click **Add** button. The following screen will pop-up.

	HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS
UPnP						
SNTP						
SNMP						
IP QoS						
Port Forwarding						
IP Filters						
LAN Clients						
LAN Isolation						
Bridge Filters						
Web Filters						
Multicast						
Static Routing						
Dynamic Routing						
Access Control						
Save All						

IP QoS Traffic Rule

Rule Name:

Source IP: Source Netmask:

Source Start Port: Source End Port:

Destination IP: Destination Netmask:

Destination Start Port: Destination End Port:

Protocol: Physical Port:

Traffic Priority:

TOS Marking: ☐ Normal Service
☐ Minimize monetary cost
☐ Maximize reliability
☐ Maximize throughput

- **Rule Name:** Enter the IP QoS session name.
- **Source IP:** Enter the Source IP Address.
- **Source Netmask:** Enter the Source IP Subnet Mask.
- **Source Start Port:** Enter the Source IP Start Port which PPP session can be activated.
- **Source End Port:** Enter the Source IP End Port which PPP session can be activated.
- **Destination IP:** Enter the Destination IP Address.
- **Destination Netmask:** Enter the Destination IP Subnet Mask.
- **Destination Start Port:** Enter the Destination IP Start Port which PPP session can be activated.
- **Destination End Port:** Enter the Destination IP End Port which PPP session can be activated.
- **Protocol:** Select the protocol from the drop down manual. The protocols supported are TCP, UDP, ICMP and ANY.
- **Physical Port:** Select the QoS Physical Port from the drop down manual.
- **Traffic Priority:** Click and select the QoS session Traffic Priority from the drop down manual.
- **TOS Marking:** Place a check at the Normal Service or select the TOS Marking from the list.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.5 ADVANCED - Port Forwarding

Port Forwarding: Port Forwarding is necessary because NAT (Network Address Translation) only forwards traffic from the Internet to the LAN if a specific port mapping exists in the NAT translation table. Because of this, the NAT provides a level of protection for computers that are connected to your LAN. However, this also creates a connectivity problem when you want to make LAN resources available to Internet clients, which you may want to do to play network games or host network applications.

Thus Port Forwarding is necessary to run certain games, chat clients, video-conferencing and other kinds of application. You might also need to configure port-forwarding if you intend to host a web server or mail server that is to be visible outside your LAN.

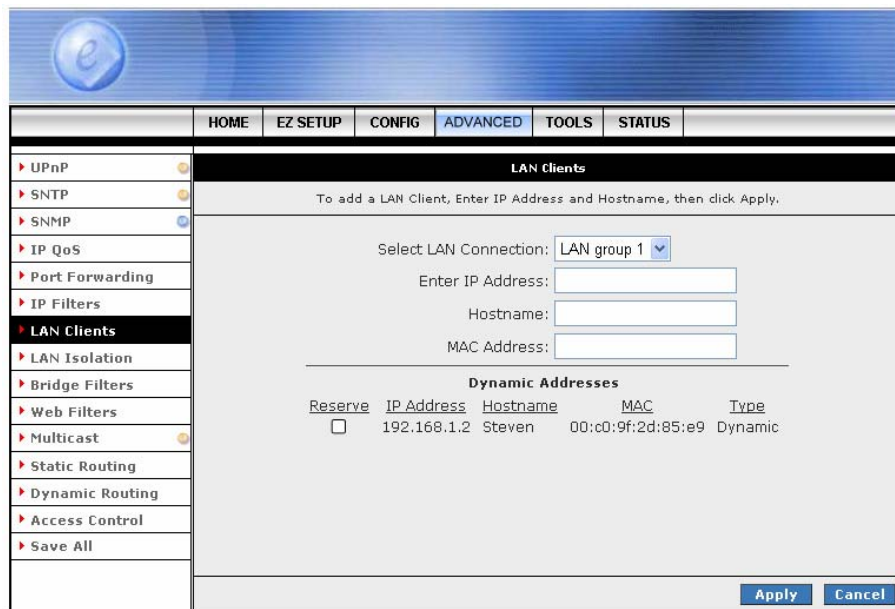
The screenshot shows the 'Port Forwarding' configuration page in a router's web interface. The interface has a blue header with a logo and a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left is a sidebar menu with various configuration options, including UPnP, SNTP, SNMP, IP QoS, Port Forwarding (selected), IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area is titled 'Port Forwarding' and contains the following fields and controls:

- WAN Connection:** A dropdown menu set to 'Hinet'.
- Allow Incoming Ping:** An unchecked checkbox.
- Select LAN Group:** A dropdown menu set to 'LAN group 1'.
- LAN IP:** A dropdown menu set to '192.168.1.2'.
- Buttons:** 'New IP', 'DMZ', and 'Custom Port Forwarding'.
- Category:** A list of radio buttons for rule categories: Games, VPN (selected), Audio/Video, Apps, Servers, and User.
- Available Rules:** A list box containing 'IPSEC L2TP' and 'PPTP'.
- Buttons:** 'Add >' and '< Remove'.
- Applied Rules:** An empty list box.
- Buttons:** 'View' and 'Apply'.

- **WAN Connection:** Select the WAN Connection profile from the drop down manual.
- **Allow Incoming Ping:** Place a check to enable the incoming ping.
- **Select LAN Group:** Select the LAN Group from the drop down manual.
- **LAN IP:** Enter the Router's LAN IP address.

- **New IP:** If you wish to manually add a LAN client so that you can apply rules to it, click on the **New IP** button. The following screen will pop-up. Refer to **ADVANCED → LAN Clients** setting for more details.

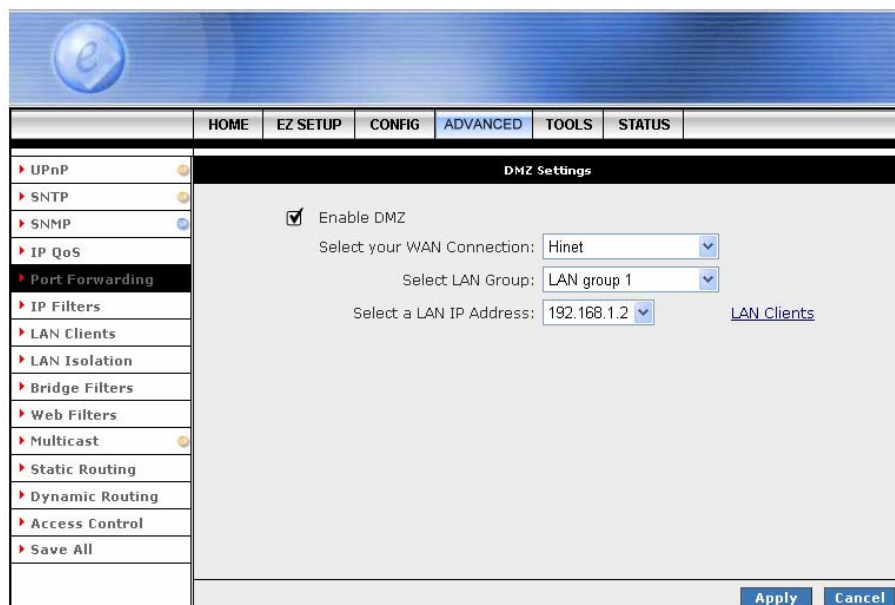
Enter the **IP Address**, **Hostname** and **MAC Address** as shown then click **Apply** to save your setting.



The screenshot shows the 'LAN Clients' configuration page. The left sidebar contains a menu with options like UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients (selected), LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area has a title bar 'LAN Clients' and a subtitle 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this, there are input fields for 'Select LAN Connection:' (set to 'LAN group 1'), 'Enter IP Address:', 'Hostname:', and 'MAC Address:'. A section titled 'Dynamic Addresses' contains a table with columns 'Reserve', 'IP Address', 'Hostname', 'MAC', and 'Type'. The table has one row with '192.168.1.2', 'Steven', '00:c0:9f:2d:85:e9', and 'Dynamic'. At the bottom right are 'Apply' and 'Cancel' buttons.

- **DMZ:** A DMZ (Demilitarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security. When there is a suspected packet coming from WAN, the firewall will forward this packet to the DMZ host.

The following screen will pop-up after clicking the DMZ button. Place a check to enable the DMZ functionality. Select the **WAN Connection**, **LAN Group** and **LAN IP Address** from the drop down manual. Click **Apply** to save and activate your setting.



The screenshot shows the 'DMZ Settings' configuration page. The left sidebar is similar to the previous one, but 'DMZ Settings' is not visible. The main content area has a title bar 'DMZ Settings' and a subtitle 'Enable DMZ'. Below this, there is a checkbox 'Enable DMZ' which is checked. There are three dropdown menus: 'Select your WAN Connection:' (set to 'Hinet'), 'Select LAN Group:' (set to 'LAN group 1'), and 'Select a LAN IP Address:' (set to '192.168.1.2'). A link 'LAN Clients' is visible next to the IP address dropdown. At the bottom right are 'Apply' and 'Cancel' buttons.

- **Custom Port Forwarding:** If there is no pre-defined Port Forwarding Rule for a particular application, a user rule can be created which defines the required Ports, Protocols and Port forwarding rules. Click the Custom Port Forwarding button and the following screen will pop-up.

The screenshot shows the 'Custom Port Forwarding' configuration window. On the left is a sidebar menu with options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding (selected), IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main area has a title bar 'Custom Port Forwarding' and a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. The configuration fields include: Connection (Hinet), Enable (checked), Application (empty), Protocol (TCP), Source IP Address (empty), Source Netmask (empty), Destination IP Address (empty), Destination Netmask (255.255.255.255), Destination Port Start (empty), Destination Port End (empty), and Destination Port Map (empty). Below these fields is a table with columns: Enabled, Name, Source IP Mask, Destination IP Mask, Port Start, Port End, Protocol, Edit, and Delete. At the bottom right are 'Apply' and 'Cancel' buttons.

To create a custom rule you will need to know the specific port number and port type that the application requires. Some applications specify a range of ports in which case you will need to know both the starting and ending port numbers in the range, which are mapped by the start port and end port fields.

The Port Map specifies the internal port that the data will be directed to on the LAN Client. When dealing with port ranges, the Internal Port will be the same as the first port in the range. When you simply want to forward a single port from outside to inside, then all three fields (Port Start, Port End and Port Map) will have the same port number.

- Available pre-defined rules are categorized according to the application type. Click the radio button adjacent to the appropriate **Category**, and then select the required application name. Click on the **Add** button to move the application into the **Applied Rules** box. To remove a rule from the Applied Rules box, select the rule and click on the **Remove** button. To complete and save the setting, click **Save All** after clicking the **Apply** button.

The screenshot shows the 'Pre-defined Rules' configuration window. It has three main sections: 'Category' on the left with radio buttons for Games (selected), VPN, Audio/Video, Apps, Servers, and User; 'Available Rules' in the center with a list of applications including Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, and Fighter Ace II; and 'Applied Rules' on the right, which is currently empty. Between the 'Available Rules' and 'Applied Rules' sections are 'Add >' and '< Remove' buttons. At the bottom of the 'Available Rules' list is a 'View' button.

4.4.6 ADVANCED - IP Filters

The **IP Filters** page allows you to specify normal Port Forwards, Block traffic to specific LAN Clients or specify Custom IP Filters that will control the flow of data across the router.

The screenshot shows the 'IP Filters' configuration page. On the left is a sidebar with a tree view containing: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, **IP Filters** (selected), LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area has a top navigation bar with: HOME, EZ SETUP, CONFIG, **ADVANCED**, TOOLS, and STATUS. Below this is the 'IP Filters' section. It includes a 'Select LAN Group' dropdown set to 'LAN group 1', a 'LAN IP' dropdown set to '192.168.1.2', and a 'New IP' button. There are two checkboxes: 'Block All Traffic' (unchecked) and 'Block Outgoing Ping' (unchecked), with a 'Custom IP Filters' link next to the second. Below these is a table with two columns: 'Category' and 'Available Rules'. The 'Category' column has radio buttons for Games, VPN, Audio/Video, Apps, Servers, and User. The 'Available Rules' column lists: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, and Fighter Ace II. There are 'Add >' and '< Remove' buttons between the columns, and a 'View' button at the bottom of the 'Available Rules' list. To the right of the table is an 'Applied Rules' section with an empty box. At the bottom right are 'Apply' and 'Cancel' buttons.

- **Select LAN Group:** Select LAN Group from the drop down manual.
- **LAN IP:** Enter the router's LAN IP Address.
- **Block All Traffic:** Click to enable blocking all traffic to specific LAN Clients.
- **Block Outgoing Ping:** Click to enable blocking all outgoing ping from LAN clients.
- **NEW IP:** Click **NEW IP** if you wish to manually add a LAN client so that you can apply rules to it.

The screenshot shows the 'LAN Clients' configuration page. The sidebar is identical to the previous screenshot. The main content area has the same top navigation bar. Below it is the 'LAN Clients' section. It starts with the instruction: 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this is a 'Select LAN Connection' dropdown set to 'LAN group 1'. There are three input fields: 'Enter IP Address:', 'Hostname:', and 'MAC Address:'. Below these is a 'Dynamic Addresses' section with a table. The table has five columns: 'Reserve', 'IP Address', 'Hostname', 'MAC', and 'Type'. There is one row with the following data: 'Reserve' is an unchecked checkbox, 'IP Address' is '192.168.1.2', 'Hostname' is 'Steven', 'MAC' is '00:c0:9f:2d:85:e9', and 'Type' is 'Dynamic'. At the bottom right are 'Apply' and 'Cancel' buttons.

- **Custom IP Filters:** Custom IP Filters allow you to specify individual rules that will deny traffic by defining the following:

- ☒ Source IP address or Source IP Subnet Mask.
- ☒ Destination IP address or Destination IP Subnet Mask.
- ☒ Port or Port range.
- ☒ Protocol.

Customer IP Filter is different from Port forwards, or Block All traffic because they allow greater scopes of IP addresses to be included in the block.

- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.7 ADVANCED - LAN Clients

LAN Client names are a way of applying specific Port-forwarding, Access Control and QoS rules to individual computers on the LAN. If DHCP is used, all DHCP clients are automatically assigned and are designated as a LAN client.

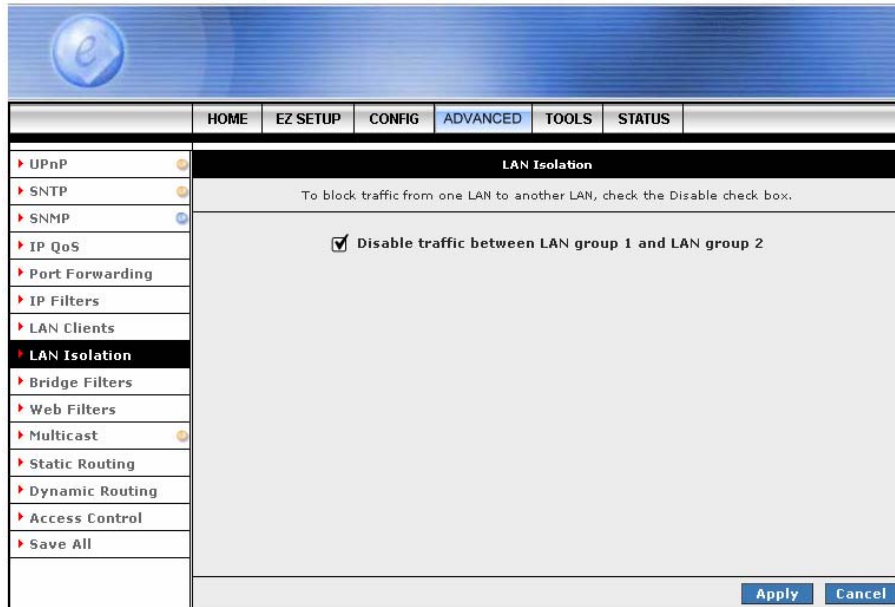
Enter the IP Address, Hostname and MAC Address as shown. To complete and save the setting, click **Save All** after clicking the **Apply** button.

The screenshot shows a web interface for configuring LAN Clients. The top navigation bar includes links for HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. A left sidebar lists various configuration options, with LAN Clients highlighted. The main content area is titled 'LAN Clients' and contains instructions: 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this, there are input fields for 'Select LAN Connection' (set to 'LAN group 1'), 'Enter IP Address', 'Hostname', and 'MAC Address'. A section titled 'Dynamic Addresses' contains a table with columns: Reserve, IP Address, Hostname, MAC, and Type. The table has one row with a checkbox in the Reserve column, the IP address 192.168.1.2, the hostname Steven, the MAC address 00:c0:9f:2d:85:e9, and the type Dynamic. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

Reserve	IP Address	Hostname	MAC	Type
☐	192.168.1.2	Steven	00:c0:9f:2d:85:e9	Dynamic

4.4.8 ADVANCED - LAN Isolation

LAN Isolation provide blocking traffic from one LAN to another LAN. Place a check at the selected rules and click **Apply** to activate your setting. To complete and save the setting, click **Save All** after clicking the **Apply** button.



The screenshot shows a web-based configuration interface for a 4 Ports ADSL2/2+ Router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left, a sidebar lists various configuration options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation (highlighted), Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area is titled "LAN Isolation" and contains the instruction: "To block traffic from one LAN to another LAN, check the Disable check box." Below this, there is a single checkbox labeled "Disable traffic between LAN group 1 and LAN group 2", which is currently checked. At the bottom right of the main area, there are "Apply" and "Cancel" buttons.

4.4.9 ADVANCED - Bridge Filters

Bridge Filtering allows packets to be forwarded or blocked, depending on the MAC address. The **Bridge Filtering** configuration page allows you to set the configuration of MAC filtering.

Bridge Filter (Or sometimes known as MAC Filter) enable rules to be defined which allow or deny data to pass through the Router based on the source and destination MAC address and data type of each data frame.

Most of the Bridge Filter Rule is to specify which computers on a network are allowed Internet access; or to determine which particular computers are allowed to access services provided by the Router.

HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS		
Bridge Filters							
☒ Enable Bridge Filters							
☒ Enable Bridge Filter Management Interface							
Select LAN: LAN group 1							
Bridge Filter Management Interface: Ethernet							
Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode		
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny		
Add							
Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete
☐	00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny	☐
Select All							
Apply						Cancel	

- **Enable Bridge Filters:** Place a tick at the check box to enable the Bridge Filters functionality. If the check box is selected, Bridge Filtering is enabled according to the list of Bridge Filter Rules that has been created. If the box is de-selected, Bridge Filtering will not be enabled, even if Bridge Filter Rules have been created.
- **Enable Bridge Filter Management Interface:** Place a check to enable the Bridge Filter Management Interface.
- **Select LAN:** Select LAN Group from the drop down manual.
- **Bridge Filter Management Interface:** Select the management interface from the drop down manual.
- **Add:** Click **Add** button to add the rule to the list of rules.
- **Edit:** To edit an existing Bridge Filter Rule, click the **Edit** radio button adjacent to the Bridge Filter Rule name.
- **Src MAC:** This is the Source MAC to block or from which to forward. The Source MAC must consist of 12 hexadecimal characters.
- **Src Port:** Select the Source Port from the drop down manual.

- **Dest MAC:** This is the Destination MAC to block or to forward to. The Destination MAC must consist of 12 hexadecimal characters.
- **Dest Port:** Select the Destination Port from the drop down manual.
- **Protocol:** Select the Protocol type for the rule from the drop down manual. Place a check to make changes to the existing Bridge Filter Rule.
- **Mode:** Select **Allow** or **Deny** for the rule.
- **Delete:** Place a check adjacent to the Bridge Filter Rule and click Apply to Delete the Bridge Filter Rule.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

☒ **Create Bridge Filter Rules:**

- Enter the Source MAC (Src MAC) and Destination MAC (Dest MAC) details.
- Select the Source Port and Destination Port from the drop down manual.
- Select the protocol type from the drop down manual. Protocol provides the choice of protocol type for the rule.
- Mode provides the choice of Allow or Deny for the rule.
- When all selections are made, click on Add to add the rule to the list of rules. A maximum of 20 MAC Filter Rules can be defined and saved.

☒ **Edit or Delete MAC Filter Rules:** To edit an existing MAC Filter Rule, click the radio button adjacent to the Filter Rule name (Edit). The Rule will then appear in the top of the MAC Filter control screen where it can be edited. When editing is complete, click Add to return the Rule to the list of existing rules.

☒ **To delete MAC Filter Rules:** click on the Delete tick box. Select All will select every rule. When the desired selections are made, effect deletion by clicking on Apply.

4.4.10 ADVANCED – Web Filters

Web Filter is a tool that has the ability to filter Internet content. Using an easy, category-based listing, you can control exactly what website content can or can not be accessed. Click the radio button to Enable or Disable the filter rules to ensure an accurate representation of the world of information reachable on the Internet.

The screenshot shows a web interface for configuring a 4 Ports ADSL2/2+ Router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left, a sidebar lists various configuration options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters (highlighted), Multicast, Static Routing, Dynamic Routing, Access Control, and Save All. The main content area is titled 'Web Filters' and contains a table of settings:

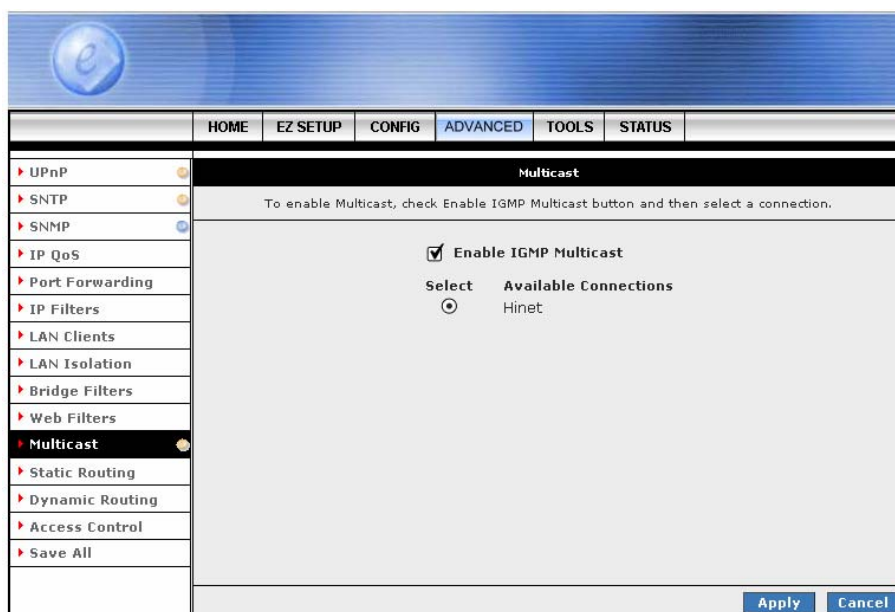
Web Filters		
Proxy	☐ Enabled	☒ Disabled
Cookies	☐ Enabled	☒ Disabled
Java Applets	☐ Enabled	☒ Disabled
ActiveX	☐ Enabled	☒ Disabled
Pop-Ups	☒ Enabled	☐ Disabled

At the bottom right of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.11 ADVANCED - Multicast

IGMP (Internet Group Management Protocol) Multicast enables communication between a single sender and multiple receivers on a network. It is used when data needs to be sent from one to many devices.



- **Enable IGMP Multicast:** Click to enable IGMP Multicast and then select a connection listed.
- **Select:** Click to select the available connection from the connection profile list.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.12 ADVANCED – Static Routing

If the Router is required to serve more than one network, you will need to set up a Static Route between the networks. Static routing can be used to allow users from one IP domain to access the Internet through the Router in another domain. A Static Route provides the defined pathway that network information must travel to reach the specific host or network which is providing Internet access.

The screenshot shows the 'Static Routing' configuration page. At the top, there is a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left, a sidebar lists various configuration options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing (selected), Dynamic Routing, Access Control, and Save All. The main content area is titled 'Static Routing'. It features a dropdown menu 'Choose a connection:' with 'Hinet' selected. Below this are input fields for 'New Destination IP:', 'Mask:' (pre-filled with '255.255.255.0'), 'Gateway:', and 'Metric:' (pre-filled with '0'). At the bottom, there is a table showing the current static route configuration.

Connection	Destination IP	Mask	Gateway	Metric	Delete
Hinet	10.0.0.6	255.255.255.0	10.0.0.2	0	☐

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

- **Configuring Static Routing:** If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Follow the following steps to create a Static Route:
 - ☑ **Choose a Connection:** Presents list of saved Connections. Select appropriate connection from the list.
 - ☑ **The New Destination IP:** Enter the address of the remote LAN network or host to which you want to assign a static route.
 - ☑ **Mask:** The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. The subnet mask defaults to 255.25.255.0
 - ☑ **Gateway:** The Gateway IP address is the IP address for the gateway device that provides contact between the gateway and the remote network.
 - ☑ **Metric:** Enter the Metric or cost for the destination.
 - ☑ **Delete:** Place a check adjacent to the rule and click Apply to Delete the rule from the list.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.13 ADVANCED – Dynamic Routing

Dynamic Routing makes use of the RIP Protocol to allow the ADSL2/2+ Router to automatically adjust to physical changes in the network. This 4 Ports ADSL2/2+ Router, using the RIP (v1 or v2) protocol, will determine the network packet route based on the fewest number of hops between the Source and the Destination. The RIP protocol regularly broadcasts routing information to other ADSL Routers on the network and is part of the IP suite.

The screenshot shows a web interface for configuring a 4 Ports ADSL2/2+ Router. The top navigation bar includes tabs for HOME, EZ SETUP, CONFIG, ADVANCED (selected), TOOLS, and STATUS. On the left, a sidebar lists various configuration options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing (highlighted), Access Control, and Save All. The main content area is titled 'Dynamic Routing' and contains the following settings:

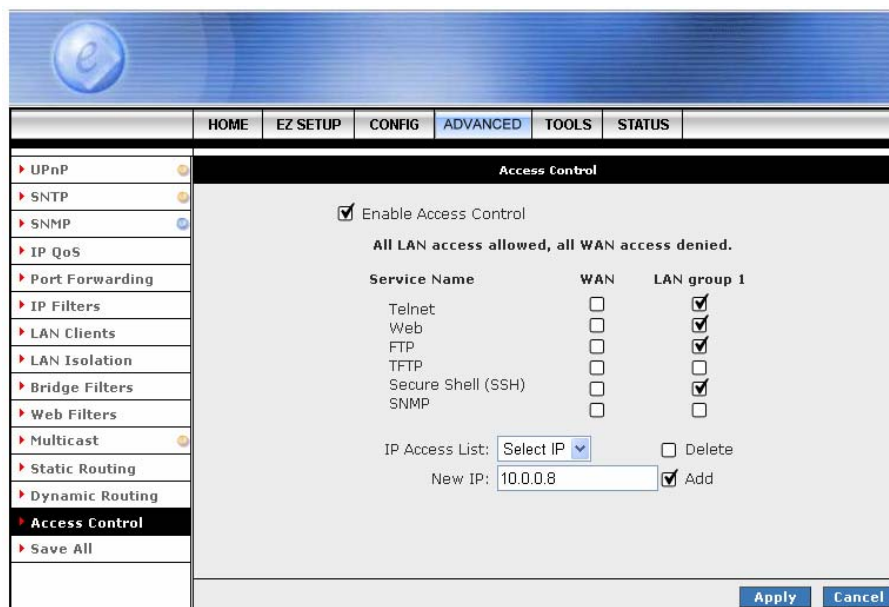
- ☒ **Enable RIP**
Protocol: RIP v2
- ☒ **Enable Password**
Password: ••••
- Interface**
LAN group 1
Hinet
- Direction**
Both
None

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

- **Enable RIP:** If this box is checked, Dynamic Routing is enabled.
- **Protocol:** Select the protocol from the drop-down manual. The choice is dependent upon the network environment. Most networks support Rip v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If Rip V2 is selected, routing data will be sent in RIP v2 format using Subnet Broadcasting. If Rip V1 Compatible is selected, routing data will be sent in RIP v2 format using Multicasting.
 - ☒ **RIPv1:** RIP Version 1: One of the first dynamic routing protocols introduced used in the Internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.
 - ☒ **RIPv2:** RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.
- **Enable Password:** Place a check to enable the entered password.
- **Direction:** Determines the direction that RIP routes will be updated.
 - ☒ **In:** the Router will only incorporate received RIP information.
 - ☒ **Out:** the ADSL Router will only send out RIP information.
 - ☒ **Both:** the ADSL Router will both incorporate received RIP information and send out updated RIP information.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.14 ADVANCED – Access Control

Use Access Control to configure advanced security functions by customizing the 4 Ports ADSL2/2+ Router. Access control enables the user to selectively direct such traffic, for example to a Web Host in the DMZ or to specific ports opened for such applications as Telnet, Web, TFTP or FTP.



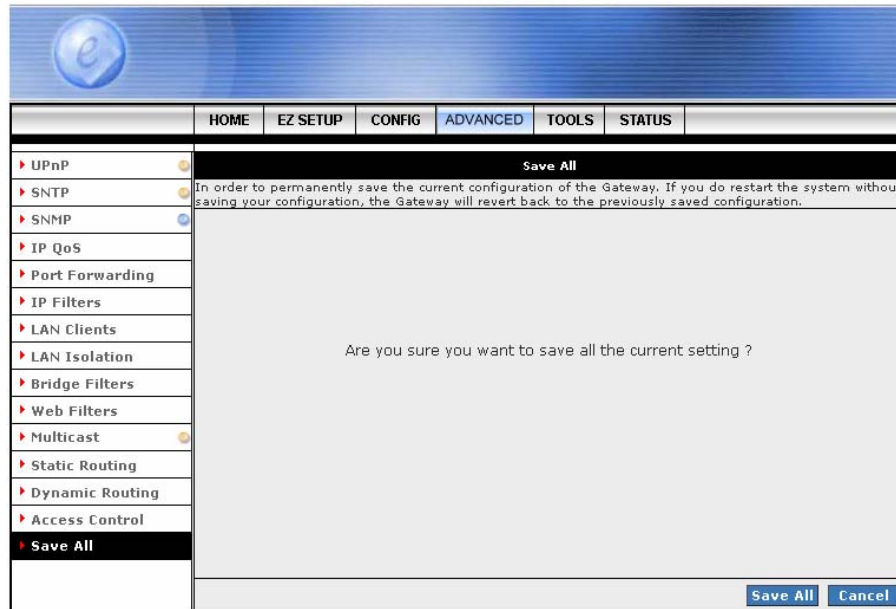
- **Enable Access Control:** Check this box to enable selective access from the WAN to your LAN for applications of the class indicated by the relevant check boxes. If Access Control is not enabled, the individual check boxes cannot be checked.
The default configuration enables Telnet, Web, FTP and SSH access from LAN to WAN. If Access Control is enabled, and an enable WAN checkbox is selected, then the WAN access to the matching service is enabled.
- **IP Access List:** This enables you to specify which LAN/WAN IP addresses are allowed access to the 4 Ports ADSL2/2+ Router configuration services specified.
- **Delete:** Delete the IP Access List from the drop down manual.
- **Add:** Add new IP Access to the list.
- **Apply:** The following dialog box will pop-up when clicking the Apply button indicates that you should not disable LAN Web Access or else you might not be able to connect to the device. Click **OK** or **Cancel** to confirm your setting.



- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.15 ADVANCED – Save All

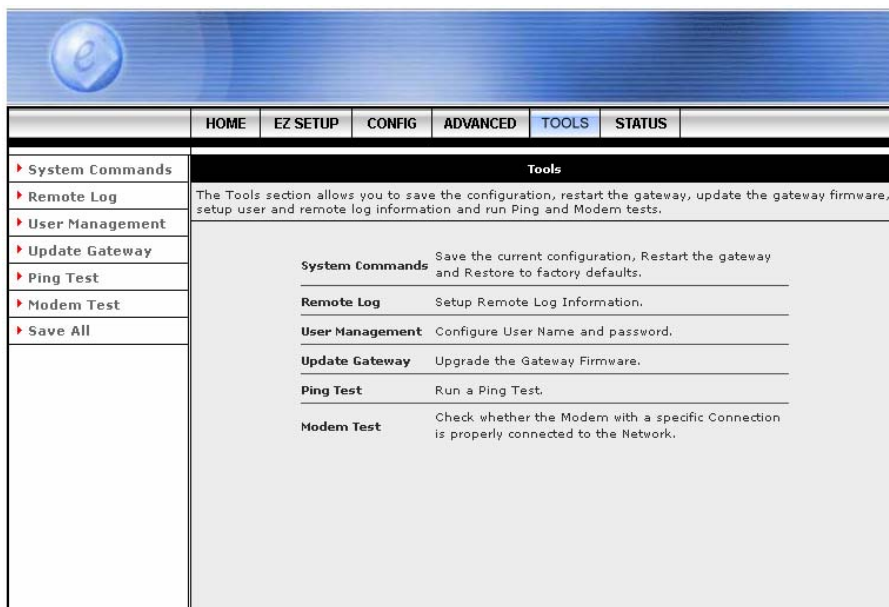
Save All: Click **Save All** in order to permanently save the current configuration of the 4 Ports ADSL2/2+ Router. If you do restart the system without saving your configuration, the 4 Ports ADSL2/2+ Router will revert back to the previously saved configuration.



- **Save All:** Click **Save All** to complete and permanently save the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.

4.5 TOOLS

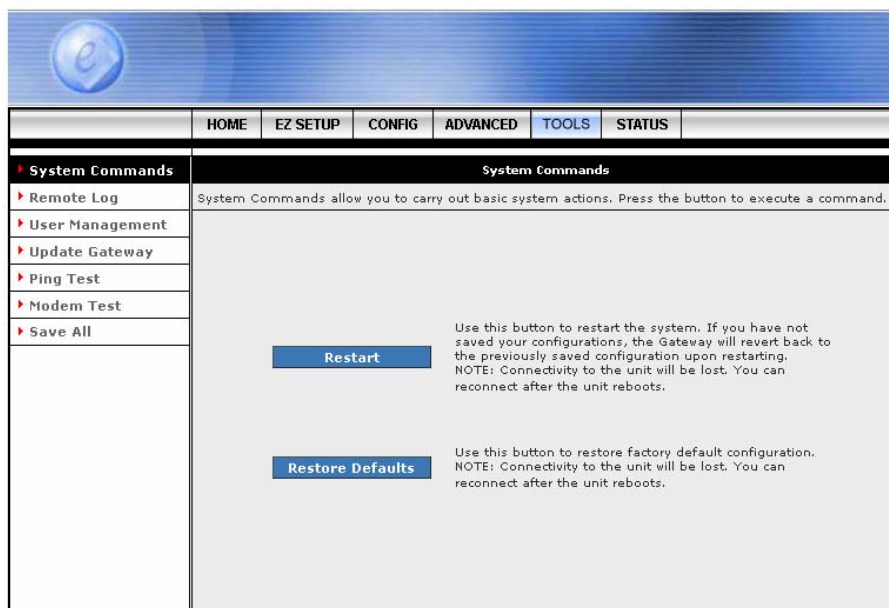
TOOLS: The **TOOLS** page allows you to save the configuration, restart the device, update the firmware/image code, setup user and remote log information and run ping/test of the 4 Ports ADSL2/2+ Router.



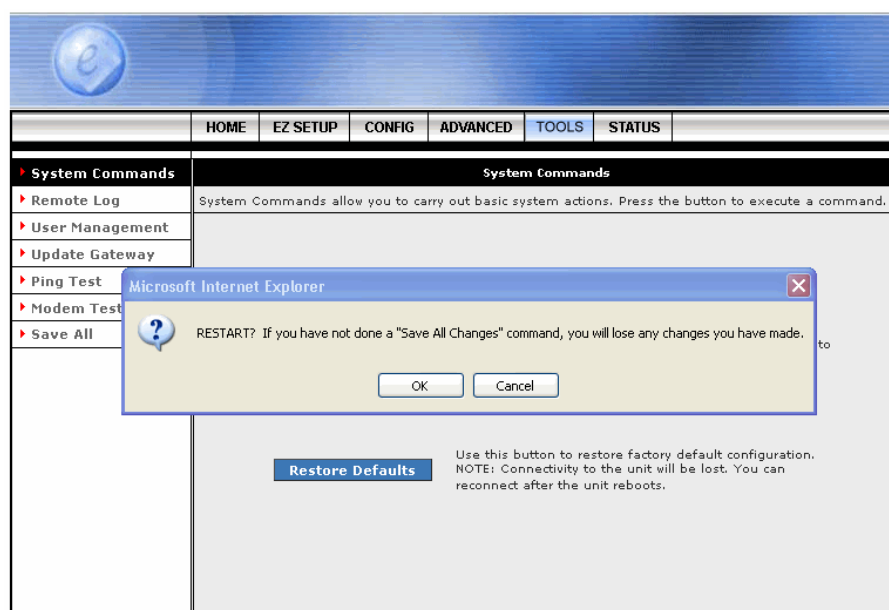
- **System Commands:** Save the current configuration, restart the 4 Ports ADSL2/2+ Router and restore to factory defaults setting.
- **Remote Log:** Setup Remote Log Information.
- **User Management:** Configure user name and password.
- **Update Gateway:** Upgrade the 4 Ports ADSL2/2+ Router firmware.
- **Ping Test:** Run a ping test.
- **Modem Test:** Check whether the modem with a specific connection is properly connected to the network.
- **Save All:** Click **Save All** to complete and permanently save the setting.

4.5.1 TOOLS - System Commands

The System Commands page allow you to carry out basic system actions.

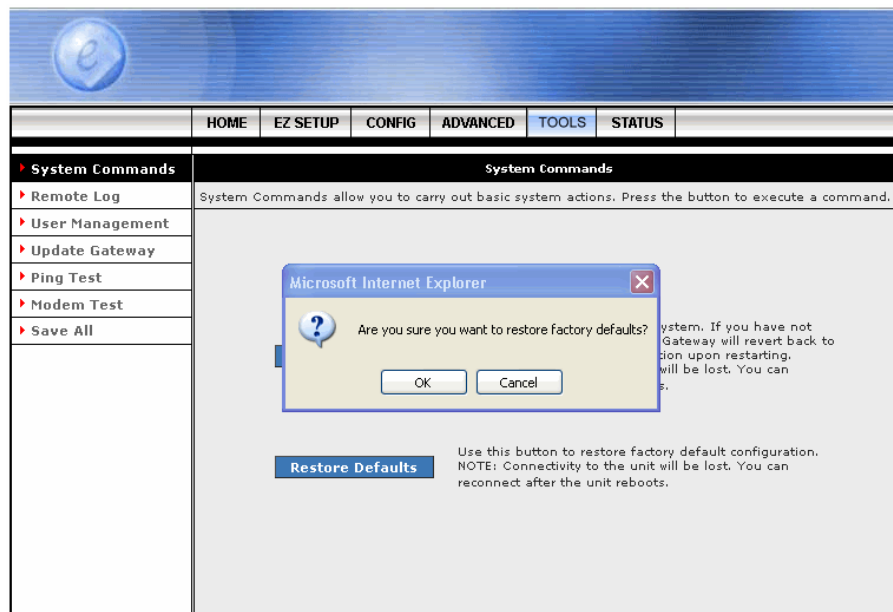


- **Restart:** Use this button to restart the 4 Ports ADSL2/2+ Router's system. The following window will pop-up. Click **OK** to confirm your setting.



NOTE: You will be redirected to the 4 Ports ADSL2/2+ Router Homepage after the unit has successfully rebooted.

- **Restore Defaults:** Use this button to restore factory default configurations. The following window will pop-up. Click **OK** to confirm your setting.



NOTE: You will be redirected to the 4 Ports ADSL2/2+ Router Homepage after the unit has successfully been restored to factory default configurations.

4.5.2 TOOLS - Remote Log

Remote Log: Using the Remote Log page, you can allow a user or users on the Internet to configure, upgrade and check the status of your 4 Ports ADSL2/2+ Router.

The screenshot shows the 'Remote Log Settings' page. At the top, there is a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS (selected), and STATUS. On the left, a sidebar menu lists: System Commands, Remote Log (selected), User Management, Update Gateway, Ping Test, Modem Test, and Save All. The main content area is titled 'Remote Log Settings' and contains the following elements:

- Log Level:** A section with a dropdown menu currently set to 'Notice'.
- Add an IP Address:** A text input field followed by an 'Add' button.
- Select a logging destination:** A dropdown menu currently set to 'None' followed by a 'Delete' button.
- Buttons:** 'Apply' and 'Cancel' buttons are located at the bottom right of the main content area.

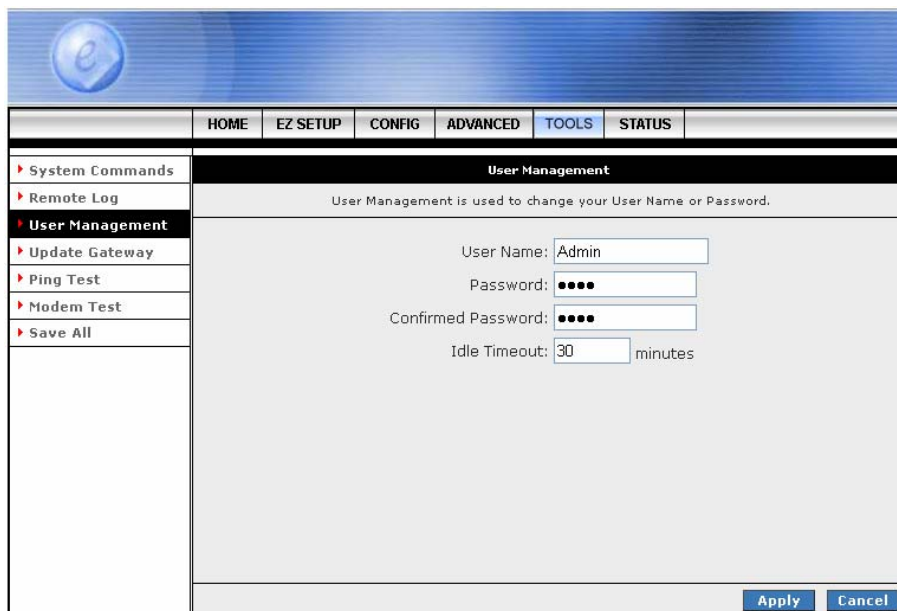
- **Log Level:** Select the Log Level from the drop down manual. The 4 Ports ADSL2/2+ Router provides the following Log Level: Panic, Alert, Critical, Error, Warning, Notice, Info and Debug.
- **Add an IP Address:** Manually enter the logging destination IP Address then click **Add** button to add your entry.
- **Delete:** Delete the logging destination IP Address from the drop down list.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.3 TOOLS - User Management

User Management: The User Management page enables you to change your User Name and/or Password. It is recommended that you change the User Name and password from the default Admin to ensure the security of the 4 Ports ADSL2/2+ Router.

For security reasons, the router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter the router User Name: **Admin** and the router Password: **Admin** to log in.

NOTE: If you forget your user name and password, access to the 4 Ports ADSL2/2+ Router can only be gained by resetting the unit to factory defaults. Pressing the “**Reset**” button for 10 seconds, the LED indicators will turn OFF and ON again indicates that the Reset process is successfully done.



The screenshot shows the 'User Management' page within the router's configuration utility. The interface has a blue header with a logo and a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS (selected), and STATUS. A left sidebar contains a tree view with options: System Commands, Remote Log, User Management (selected), Update Gateway, Ping Test, Modem Test, and Save All. The main content area is titled 'User Management' and contains the text: 'User Management is used to change your User Name or Password.' Below this, there are four input fields: 'User Name:' with the value 'Admin', 'Password:' with masked characters '....', 'Confirmed Password:' with masked characters '....', and 'Idle Timeout:' with the value '30' and the unit 'minutes'. At the bottom right of the main area are two buttons: 'Apply' and 'Cancel'.

- **User Name:** Enter the user specify User Name
- **Password:** Enter the user specify Password.
- **Idle Timeout:** For security, the administrator's login to the router configuration will timeout after a period of inactivity.
- **Apply:** Click the Apply button to confirm your setting.
- **Cancel:** Click Cancel to ignore all the changes.
- **Save All:** To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.4 TOOLS - Update Gateway

Update Gateway: Firmware is the software that controls the 4 Ports ADSL2/2+ Router and also provides the user interface that is subject of this manual. The Firmware resides in the 4 Ports ADSL2/2+ Router internal Flash memory; currently loaded firmware version can be found under **STATUS → Product Information**.

Note: It is recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you may need to restore your configuration settings.

To access Firmware Updates, click on **TOOLS → Update Gateway**. The following window screen will pop-up.

	HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS
System Commands	Update Gateway					
Remote Log	To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.					
User Management						
Update Gateway						
Ping Test						
Modem Test						
Save All						
	Select a File: Browse... (Max file size 3.5 MB) Firmware Image can be the combined single image with or without digital signature. Update Gateway The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup. Get Configuration Status: None					

- **Select a File:** Click on the **Browse...** button to locate the Firmware or update image file from your computer's hard drive.
- **Update Gateway:** Click the **Update Gateway** button to upgrade your 4 Ports ADSL2/2+ Router. The system will be restarted automatically after the Firmware/Image is successfully uploaded. You will need to reconnect again to configure your setup.
- **Get Configuration:** You may download your configuration file from the system by clicking **Get Configuration**. Follow the instruction and save your configuration file in your hard drive.

The following screen will pop-up when clicking the **Update Gateway** button. Click **Browse...** button to locate the configuration file or update image file from your computer's hard drive then click **Update Gateway**. After the configuration file upgrade process, click **Restart Gateway** to activate your previous setting.

Update Gateway

To update your gateway firmware, choose an update image or configuration file in Select a File, and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.

Select a File:

(Max file size 3.5 MB)

The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.

Try the right upgradable file and in case of failure or on success RESTART the gateway.

Status: File does not contain the checksum

- **Select a File:** Click on the **Browse...** button to locate the configuration file from your computer's hard drive.
- **Update Gateway:** Click the **Update Gateway** button to upgrade your configuration file.
- **Restart Gateway:** Click **Restart Gateway** after the upgrade process to activate your setting.

Note: When uploading Firmware/Configuration File to the 4 Ports ADSL2/2+ Router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the upgrading process. When the upload is complete, your 4 Ports ADSL2/2+ Router will automatically reboot and restart. The upgrade process will typically take about 1~2 minutes.

4.5.5 TOOLS - Ping Test

Ping Test: The Ping Test page provides an easy way to ping the 4 Ports ADSL2/2+ Router without invoking the command line interface.

The screenshot shows a web interface for a 4 Ports ADSL2/2+ Router. At the top is a blue header with a logo. Below it is a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS (selected), and STATUS. On the left is a sidebar menu with options: System Commands, Remote Log, User Management, Update Gateway, Ping Test (selected), Modem Test, and Save All. The main content area is titled 'Ping Test' and contains the following fields and controls:

- Enter IP Address to ping:
- Packet size: bytes
- Number of echo requests:
-

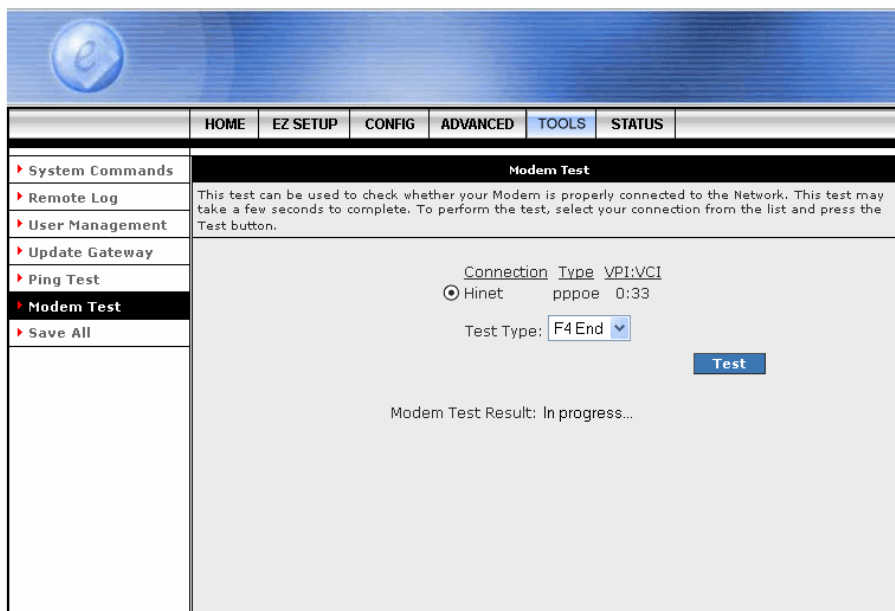
Below these fields is a text area displaying the results of the ping test:

```
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255
time=0.0 ms
--- 192.168.1.1 ping statistics ---
```

- **Enter IP Address to ping:** Enter the IP Address to ping.
- **Packet size:** Enter the packet size in bytes.
- **Number of echo requests:** Enter the number of echo request.
- **Test:** Click Test to start the ping test. The result will be shown in the window underneath.

4.5.6 TOOLS - Modem Test

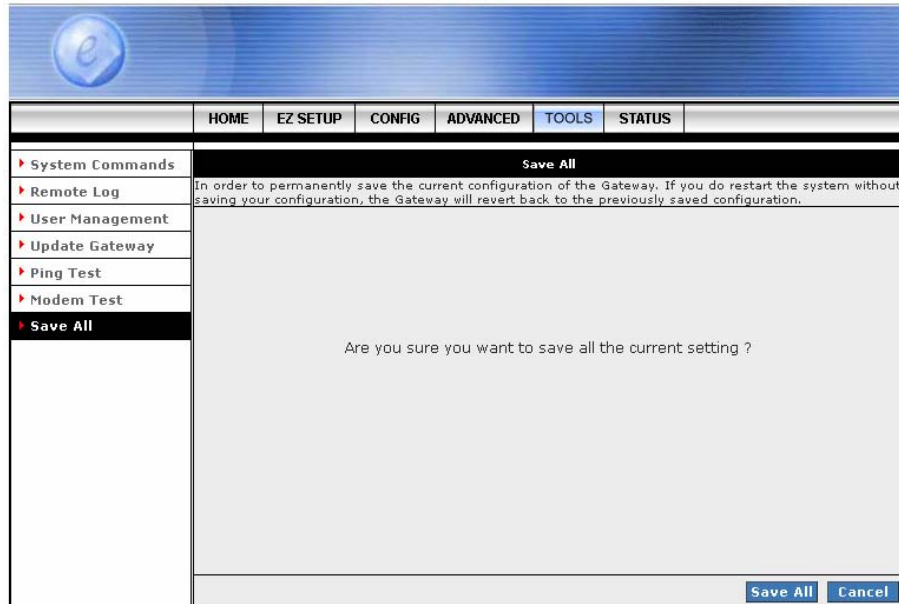
Modem Test: The Modem Test page can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the **Test** button. The value returned will either be **Success** or **Fail**.



The screenshot shows a web interface for a router. At the top is a blue header with a logo. Below it is a navigation bar with tabs: HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS (selected), and STATUS. On the left is a sidebar menu with options: System Commands, Remote Log, User Management, Update Gateway, Ping Test, Modem Test (highlighted), and Save All. The main content area is titled 'Modem Test' and contains a description: 'This test can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button.' Below this, there are fields for 'Connection' (radio button selected for 'Hinet'), 'Type' (dropdown menu showing 'VPI:VCI'), and 'Test Type' (dropdown menu showing 'F4End'). A blue 'Test' button is located to the right of the Test Type dropdown. At the bottom, it says 'Modem Test Result: In progress...'.

4.5.7 TOOLS – Save All

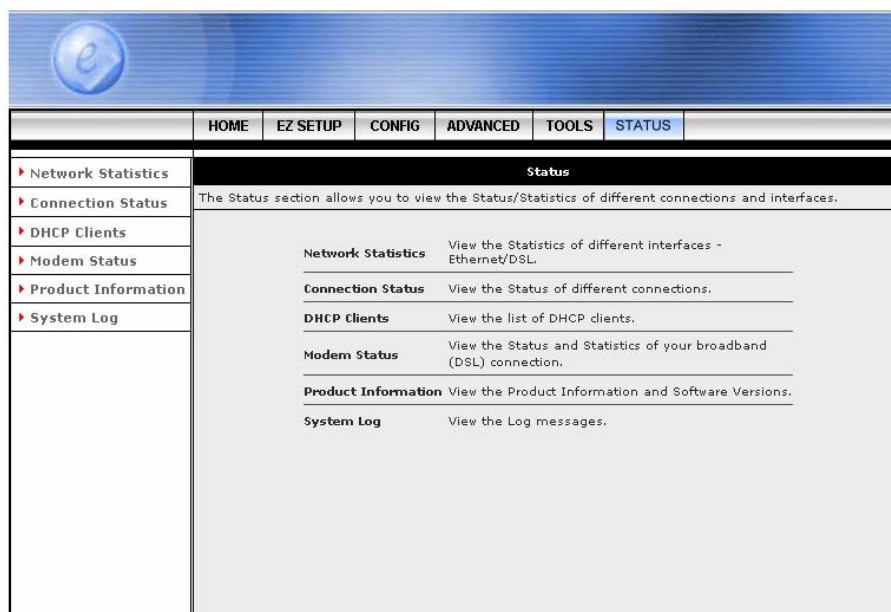
Save All: Click **Save All** in order to permanently save the current configuration of the 4 Ports ADSL2/2+ Router. If you do restart the system without saving your configuration, the 4 Ports ADSL2/2+ Router will revert back to the previously saved configuration.



- **Save All:** Click **Save All** to complete and permanently save the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.

4.6 STATUS

The Status Menu provides a dynamically-updated information about your 4 Ports ADSL2/2+ Router's Network Status, Connection Status, Modem Status and device performance.



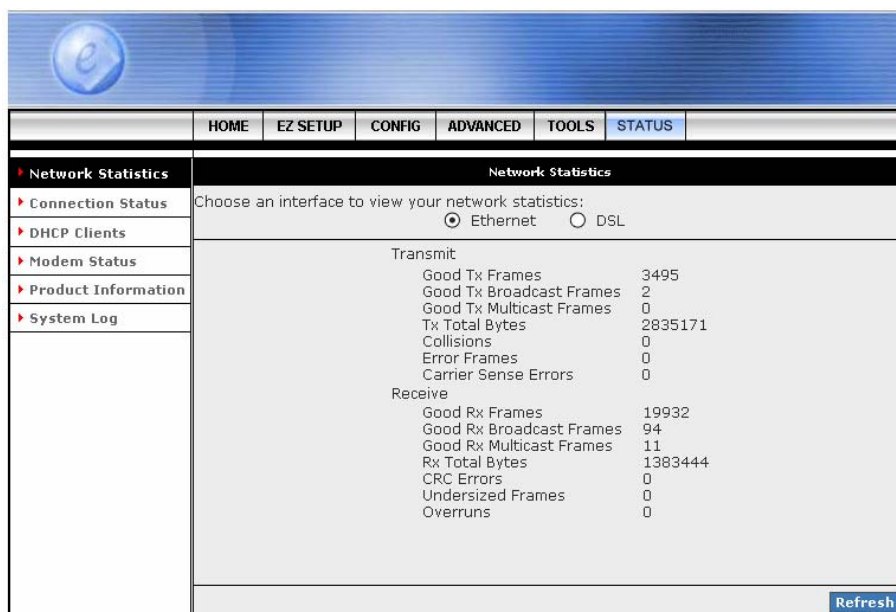
- **Network Statistics:** View the Statistics of different interfaces - Ethernet/USB/ADSL.
- **Connection Status:** View the Status of different connections.
- **DHCP Clients:** View the list of DHCP clients.
- **Modem Status:** View the Status and Statistics of your broadband (DSL) connection.
- **Product Information:** View the Product Information and Software Versions.
- **System Log:** View the Log messages.

4.6.1 STATUS - Network Statistics

The Network Statistics show the Select Network Interface type to peruse statistics for each type of connection. Click Ethernet, USB(Optional) or DSL to view your Network Statistics.

4.6.1.1 STATUS - Network Statistics - Ethernet

Ethernet: Shows the Transmit/Receive Frames, Error Frames, Collision and CRC Errors information of the Ethernet Interface. The traffic counter will reset if the device is rebooted.

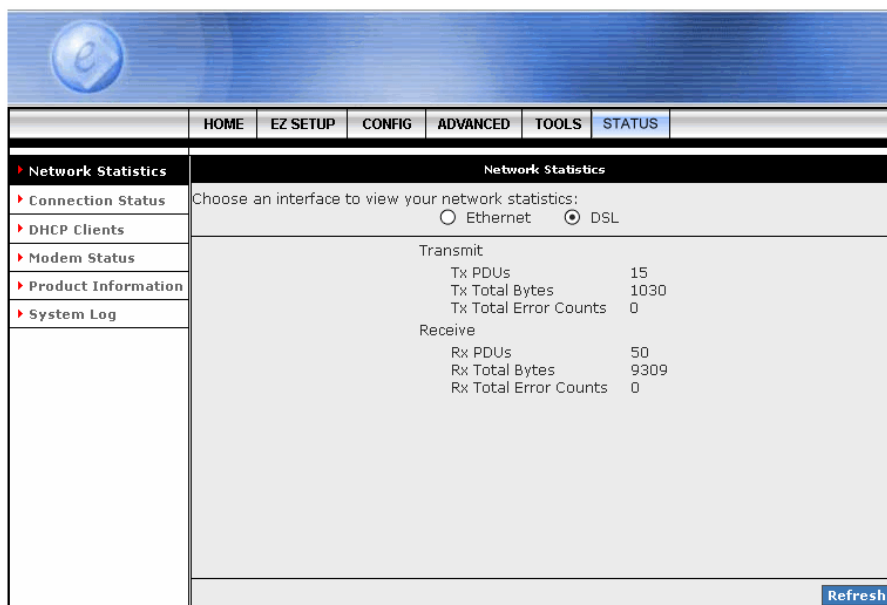


	HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS
Network Statistics	Network Statistics					
Connection Status	Choose an interface to view your network statistics:					
DHCP Clients	☒ Ethernet ☐ DSL					
Modem Status	Transmit					
Product Information	Good Tx Frames 3495					
System Log	Good Tx Broadcast Frames 2					
	Good Tx Multicast Frames 0					
	Tx Total Bytes 2835171					
	Collisions 0					
	Error Frames 0					
	Carrier Sense Errors 0					
	Receive					
	Good Rx Frames 19932					
	Good Rx Broadcast Frames 94					
	Good Rx Multicast Frames 11					
	Rx Total Bytes 1383444					
	CRC Errors 0					
	Undersized Frames 0					
	Overruns 0					
	Refresh					

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.1.2 STATUS - Network Statistics - DSL

DSL: Shows the Total Bytes Receive/Transmit and Error Count information of the ADSL (WAN) Interface. The traffic counter will reset if the device is rebooted.



The screenshot shows a web interface for a 4 Ports ADSL2/2+ Router. The top navigation bar includes links for HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. The left sidebar contains a menu with options: Network Statistics, Connection Status, DHCP Clients, Modem Status, Product Information, and System Log. The main content area is titled 'Network Statistics' and displays a selection for the interface: Ethernet (unselected) and DSL (selected). Below this, the statistics are divided into Transmit and Receive sections. The Transmit section shows 15 Tx PDUs, 1030 Tx Total Bytes, and 0 Tx Total Error Counts. The Receive section shows 50 Rx PDUs, 9309 Rx Total Bytes, and 0 Rx Total Error Counts. A Refresh button is located at the bottom right of the statistics area.

Network Statistics	
Choose an interface to view your network statistics: ☐ Ethernet ☒ DSL	
Transmit	
Tx PDUs	15
Tx Total Bytes	1030
Tx Total Error Counts	0
Receive	
Rx PDUs	50
Rx Total Bytes	9309
Rx Total Error Counts	0
Refresh	

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.2 STATUS – Connection Status

The Connection Status page display status of the current active connection.



HOME

EZ SETUP

CONFIG

ADVANCED

TOOLS

STATUS

▶ Network Statistics

▶ **Connection Status**

▶ DHCP Clients

▶ Modem Status

▶ Product Information

▶ System Log

Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
Hinet	pppoe	218.167.38.148	Connected	0hr 0min 34sec	N/A

Refresh

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.3 STATUS - DHCP Clients

The DHCP Clients page shows the MAC Address, IP Address, Host Name and Lease Time for each DHCP client connected to the 4 Ports ADSL2/2+ Router.



HOME

EZ SETUP

CONFIG

ADVANCED

TOOLS

STATUS

▶ Network Statistics

▶ Connection Status

▶ DHCP Clients

▶ Modem Status

▶ Product Information

▶ System Log

DHCP Clients (1)

Select LAN: LAN group 1

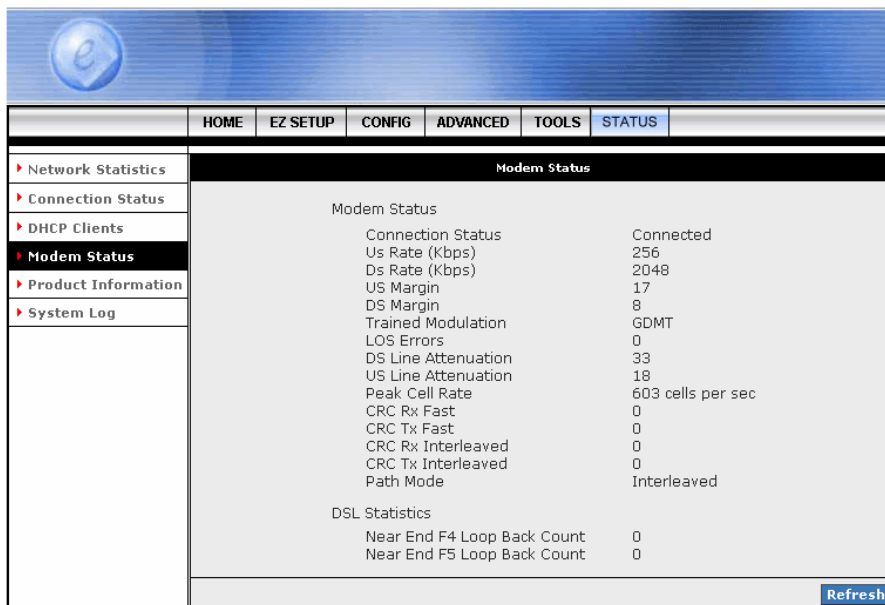
MAC Address	IP Address	Host Name	Lease Time
00:c0:9f:2d:85:e9	192.168.1.2	Steven	0 days 0:41:12

Refresh

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.4 STATUS - Modem Status

The **Modem Status** page shows the 4 Ports ADSL2/2+ physical layer or link status. The information displayed on this page is either inherent to the 4 Ports ADSL2/2+ Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user.

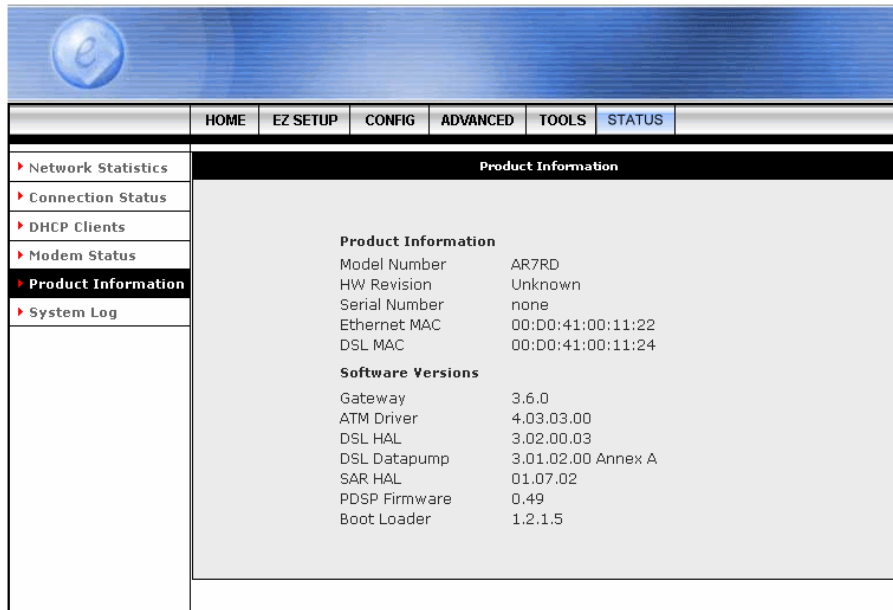


	HOME	EZ SETUP	CONFIG	ADVANCED	TOOLS	STATUS	
▸ Network Statistics	Modem Status						
▸ Connection Status	Modem Status						
▸ DHCP Clients	Connection Status Connected						
▸ Modem Status	Us Rate (Kbps) 256						
▸ Product Information	Ds Rate (Kbps) 2048						
▸ System Log	US Margin 17						
	DS Margin 8						
	Trained Modulation GDMT						
	LOS Errors 0						
	DS Line Attenuation 33						
	US Line Attenuation 18						
	Peak Cell Rate 603 cells per sec						
	CRC Rx Fast 0						
	CRC Tx Fast 0						
	CRC Rx Interleaved 0						
	CRC Tx Interleaved 0						
	Path Mode Interleaved						
	DSL Statistics						
	Near End F4 Loop Back Count 0						
	Near End F5 Loop Back Count 0						
	Refresh						

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.5 STATUS - Product Information

The **Product Information** show the complete information and various parameters of the 4 Ports ADSL2/2+ Router including Software Versions.



The screenshot shows the web interface of a 4 Ports ADSL2/2+ Router. The top navigation bar includes links for HOME, EZ SETUP, CONFIG, ADVANCED, TOOLS, and STATUS. The left sidebar contains a list of status-related items: Network Statistics, Connection Status, DHCP Clients, Modem Status, Product Information (selected), and System Log. The main content area displays the Product Information page, which is divided into two sections: Product Information and Software Versions.

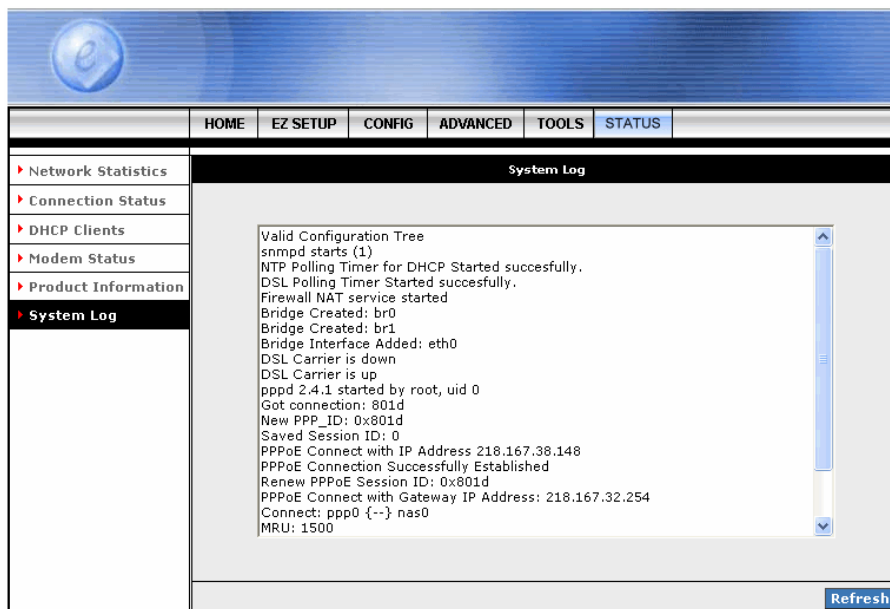
Product Information	
Product Information	
Model Number	AR7RD
HW Revision	Unknown
Serial Number	none
Ethernet MAC	00:D0:41:00:11:22
DSL MAC	00:D0:41:00:11:24
Software Versions	
Gateway	3.6.0
ATM Driver	4.03.03.00
DSL HAL	3.02.00.03
DSL Datapump	3.01.02.00 Annex A
SAR HAL	01.07.02
PDSP Firmware	0.49
Boot Loader	1.2.1.5

- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

4.6.6 STATUS - System Log

The **System Log** page shows the events triggered by the system. Click System Log to access the 4 Ports ADSL2/2+ Router's System Log information.

This page contains information that is dynamic and will refresh every 5~10 seconds..



- **Refresh:** Click **Refresh** button to reload Web browser. Changes may have occurred, but the Web browser may be caching the old configuration.

Appendix A: Router Terms

What is a firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The router provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.

Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The router contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate" the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the router. The router "fakes" the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

Appendix B: Helps

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients and PPP Connection.

1. **Firewall:** Help for Port Forwarding, Access Control, and Advanced Security.

■ **NAT and Firewall service (Section 4.3.3 : LAN Setup - Firewall/NAT Services)**

The DSL Router uses Network Address Translation (NAT) and Stateful Packet Inspection (SPI) Firewall to protect your home network. The NAT and Firewall Service can be globally (for LAN and all WAN connections) disabled/enabled from the Setup Firewall/NAT Service page. If disabled no NAT functionality nor firewall protection can be provided. For each WAN connection (e.g. the Internet connection) NAT and Firewall (SPI) can be enabled/disabled. With Firewall (SPI) enabled on a WAN connection all incoming packets are examined by the Stateful Packet Inspection engine and traffic is dropped if it is not matching an existing connection opened from LAN side or a port forwarding rule. Connections from LAN side to the Internet are trusted and allowed to pass thru the router unless explicit IP Filter rules are used to block the LAN traffic. This Asymmetric Permissive Firewall setup (drop from WAN, allow from LAN) provides easy to use Internet access while protecting the home network.

■ **Port Forwarding (Section 4.4.5 : ADVANCED - Port Forwarding)**

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. To configure a service, game or other application select the external connection (for example the Internet connection), select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for your application. You can also add/edit/delete rules without using the pre-defined Firewall Policy Database (games, services, etc.). Click on **Custom Rules** to access this type of interface. In the presence of the firewall, anonymous Internet traffic is blocked.

■ **IP Filters (Section 4.4.6 : ADVANCED - IP Filters)**

This firewall feature allows you to block network access based on a user's computer IP address. You can use this page to block specific traffic (for example block web access) or any traffic from a computer on your local network. To configure an IP Filter rule select the computers' IP address and add the corresponding firewall traffic definition from the Firewall Policy Database. If the traffic type is set to "Any" all network traffic from that computer will be blocked. You can also add/edit/delete IP Filter rules without using the pre-defined Firewall Policy Database (games, services, etc.). Click on "Custom Rules" to access this type of interface.

■ **Access Control (Section 4.4.14 : ADVANCED – Access Control)**

Open the access from the Internet (WAN) or LAN to the router's management ports (web, telnet, ssh, ftp, tftp, snmp). There are security risks associated with this action. For this reason remote management is restricted to computers on the network specified in the IP Access Control List that can hold up to 16 IP addresses. The Access Control List provides a global enable/disable that will enable or disable the ACL. If the ACL is disabled, the default behavior (i.e. DENY on the WAN, Accept on the LAN is enabled for all IP addresses) is enforced. If no IP addresses are specified within the ACL, the ACL will be will act as if it is disabled until the first IP address is added.

■ **DMZ (Section 4.4.5 : ADVANCED - Port Forwarding)**

Setting a computer on your local network as DMZ forwards any network traffic that is not redirected to another computer via the port forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet.

■ **PING (Section 4.5.5 : TOOLS - Ping Test)**

Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the router to respond to a ping from the Internet. Blocking outgoing ping (ICMP) (IP Filters page) generated from a particular LAN IP can be used if your PC has a virus that attempts a Ping-of-Death Denial of Service attack.

2. **Bridge Filters (Section 4.4.9 : ADVANCED - Bridge Filters):** Help section for Bridge Filters.

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the each defined filter rules sequentially, and when a matched is determined, the appropriate filtering action (determined by the access type selected ... i.e allow or deny) is performed. The user should note that the bridge filter will only examined frames from interfaces which is part of the bridge itself. Twenty filter rules are supported with bridge filtering.

The User Interface for Bridge Filter allows the user to add/edit/delete, as well as, enable the filter rules. To add a rules, simply define the source MAC address, destination MAC address and frame type with desired filtering type (i.e. allow/deny), and press the **Add** button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as **don't care**. Blanks can be used in the MAC address space, and would be considered also as **don't care**.

To edit/modify an existing filter rule, select the desired rule created previously from "**Add**" in the "**Edit**" select box. The selected filter rule will appear on top section, as with the "**Add**" filter rule. Make the desired change to the MAC address, frame type and/or access type, and press "**Apply**".

To delete filter rule(s), select the filter rule entry to delete in the "**Delete**" selection box. Note that multiple deletion is possible. Once all the desired filter rule(s) is/are selected for deletion, press the

"Apply" button. The **"Select All"** select box can also be used to delete all the filter rule. It provides a quick method of selecting all filter rules for deletion.

The **"Enable Bridge Filters"** button allow the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the **"Apply"** button.

Note: There are three hidden filter rules within the bridge filter table. These rules are entered automatically by the system to ensure the user does not **"lock"** themselves out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

3. **LAN Clients (Section 4.4.7 : ADVANCED - LAN Clients):** Help section for LAN Clients.

Using this feature user can see all the PCs on the LAN segment. Each PC is qualified to be either **"dynamic"** (PC obtained a lease from this router) or **"static"** (PC has a manually configured IP address).

User can add a **"static"** IP address(belonging to the network segment of the router LAN IP address). Any existing static entry falling within DHCP server's range can be deleted and the IP address would be made available for future allocation.

Once an IP address is allocated it shows up in the list of LAN clients as a **"dynamic"** entry. Any dynamic entry can be converted into static by using **"reserve"** checkbox.

Note: Dynamic clients show up in the list only when DHCP server is running.

4. **PPP Connection (Section 4.3.1.1 : CONFIG - WAN Setup – New Connection):** Help for establishing a PPP Connection.

Username: The username for the DSL access.

Password: The password for the DSL access.

Authentication: Specifies the authentication protocol required to establish connection.

On-Demand: Enable on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.

Idle Timeout: Specifies that DSL should disconnect if the link has no activity detected for n seconds. A non-zero value.

Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. A non-zero value.

Set Defaultroute: Specify connection as the default-route.

MRU: Maximum Receive Unit the DSL connection can receive. It is an negotiated value that ask the provider to send packets of no more than n bytes. The minimum MRU value is 128.

Enforce MRU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.

Debug: Enables PPP connection debugging facilities.

Connect: Use the current settings to establish a ppp connection. In "On Demand" mode "Connect" takes no action in establishing connection.

Disconnect: Disconnects the ppp connection.

5. **UPnP (Section 4.4.1 : ADVANCED – UPnP):** Help pages for UPnP.

- UPnP NAT and Firewall Traversal allow traffic to pass-thru the router for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over which the incoming traffic will be present, for example the default Internet connection.

6. **IP QoS (Section 4.4.4 : ADVANCED - IP QoS):** Help section for IP QoS.

- IP QoS services in the NSP is applicable to the output device (Egress side). Meaning the IP QoS traffic shaping is associated with any transmitted traffic from the perspective of the NSP. Each output device has 3 priority queues associated with transmit data. The High priority queue has strict priority over medium and low priority queues. The Medium and Low priority queues are serviced on a Round Robin priority basis according to the configured weights (WRR), after the High priority queue has been completely serviced.

The "**IP QoS**" section under "**Advanced section**" allows you to setup IP QoS for a connection. The "**IP QoS**" section has two sub-sections - **QoS Setup Page** and **Rule Setup Page**.

- **QoS Setup Page**

The QoS setup page allows you to configure IP QoS for a connection, to view the configured QoS rules and to add/delete a QoS rule.

Choose a connection: This field allows you choose a connection from the list of available connections. For e.g. choose a WAN connection to enable IP QoS for the Upstream traffic of the Modem. On the other hand choose the LAN connection (Ethernet and USB Bridged) for the downstream traffic.

Low/Medium priority weights: These 2 fields will allow you to select the weights of the Medium and Low priority queues in increments of 10 percent, so that that the sum of the weights of these 2 queues is equal to 100 percent.

Enable IP QoS: This field allows you to enable/disable IP QoS for the chosen connection.

Trusted Mode: The NSP has two primary modes of operation with regard to queue traffic prioritization - Trusted and Un-trusted. This field allows you to choose the mode - Trusted (checked) and Un-trusted (Unchecked).

In "**Trusted mode**" all the rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. The "**Un-trusted**" mode will match first against all rules as in "**Trusted**" mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority - Low.

Rules section: This section displays a list of configured rules, allows you to add a new rule and allows you to delete an existing rule.

Each rule is a Matching criteria that identifies an Application traffic to be transmitted by the NSP using one of the 3 Priority Queues - High, Medium and Low.

Note: If IP QoS is enabled and no rules are defined, a Default Rule is added which is hidden. The Default Rule puts all the Traffic to be transmitted in the **Low Priority Queue**.

■ Rule Setup Page

This page is invoked when you click on the "**Add**" button of "**QoS Setup Page**". This page allows you add a Rule or Matching criteria that identifies an Application traffic. The Application traffic can be identified by Rule Name, Source/Destination IP Address and Netmask, Source/Destination Port range, Protocol and Traffic Priority.

The Traffic Priority field corresponds to the Priority Queue (High/Medium/Low) for for this traffic. The possible options for Protocol are - ANY, ICMP, TCP and UDP. Wildcard(*) entries are allowed for IP Address/Netmask and Port range fields.

The additional TOS marking field allows you to assign a TOS value to this traffic. The values for the TOS marking can be - No Change, Normal Service, Minimize monetary cost, Maximize reliability, Maximize throughput and Minimize delay.

Appendix C: Frequently Asked Questions

The Frequently Asked Questions addresses common questions regarding 4 Ports ADSL2/2+ Router settings. Some of these questions are also found throughout the guide, in the sections to which they reference.

1. How do I determine if a link between the Ethernet card (NIC) and the 4 Ports ADSL2/2+ Router has been established?

Ans. A ping test would determine if a connection is established between your 4 Ports ADSL2/2+ Router and computer. Using, the ping command, ping the IP address of the 4 Ports ADSL2/2+ Router, in this case, 192.168.1.1 (default). For more information on Ping Testing, refer to Appendix C: Troubleshooting Guide. Alternatively, if the Ethernet LINK LED is solidly on, then the Ethernet link is established.

2. How do I determine if a link between the 4 Ports ADSL2/2+ Router and the Internet has been established?

Ans. Similar to the previous question, a ping test would determine whether or not a connection is established. However, this time use a URL instead of an IP Address, such as www.paradigm.com.tw. Alternatively, if the ADSL LED is solidly on, then the ADSL link is established.

3. How can I find/verify my 4 Ports ADSL2/2+ Router and/or computer Ethernet MAC Address?

Ans. Refer to Chapter 3, Section 3.4 for details.

4. What is MAC Address?

Ans. Short for **Media Access Control Address**. It is a hardware address that uniquely identifies each node of a Ethernet networking device. This address is usually permanent.

5. What is NAT (Network Address Translation) and what is it used for?

Ans. NAT translates multiple IP Address on the private LAN to one public IP Address (in WAN) that is sent out to the Internet. NAT adds a level security since the IP address of a PC connected to the private LAN is never transmitted on the Internet.

6. What can I do when I am not able to get the web configuration screen for this 4 Ports ADSL2/2+ Router?

Ans. Remove the proxy settings on your Internet Browsers or remove the dial-up settings on your browser.

7. What is DMZ (DeMilitarized zone)?

Ans. DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ features.

8. What is the maximum IP addresses supported by this 4 Ports ADSL2/2+ Router?

Ans. The 4 Ports ADSL2/2+ Router can support up to 253 IP addresses.

Appendix D: Troubleshooting Guide

The Troubleshooting Guide provides answers to common problems regarding the 4 Ports ADSL2/2+ Router settings, connections, and computer settings.

1. The 4 Ports ADSL2/2+ Router does not work (None of the LEDs light up)

Ans. Check the following:

1. Make sure that the 4 Ports ADSL2/2+ Router is plugged into a power socket.
2. Make sure that you are using the correct power supply for your 4 Ports ADSL2/2+ Router device.
3. Make sure the power switch on the 4 Ports ADSL2/2+ Router is turned on

2. I changed the LAN IP Address in the LAN configuration page and my PC is no longer able to detect the 4 Ports ADSL2/2+ Router.

Ans. After changing the LAN IP Address of the 4 Ports ADSL2/2+ Router, proceed to the following step before a PC is able to recognize the 4 Ports ADSL2/2+ Router:

1. Click **"Start"** → **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.
3. In the command prompt, type **"ipconfig/release"** then press **"Enter"**.
4. Type **"ipconfig / renew"** then press **"Enter"**.

3. LAN (Link/Act) LED does not light up.

Ans. Check the following:

1. Make sure that the LAN cables are securely connected to the 10/100Base-T port.
2. Make sure that you are using the correct cable type for your Ethernet equipment.
3. Make sure the computer's Ethernet port is configured for auto-negotiation.

4. Failed to configure the 4 Ports ADSL2/2+ Router through web browser (By a client PC in LAN)

Ans. Check the following:

1. Check the hardware connection of the 4 Ports ADSL2/2+ Router's LAN port. The LED will lit when a proper connection is made.
2. Check your Windows TCP/IP setting (Refer to Chapter 3 for setting details).
3. Open the Windows System Command Prompt:
 - For Windows 9x/ME: Manually enter **winipcfg**, then press **Enter**.
 - For Windows 2000/XP: Manually enter **ipconfig/all**, then press **Enter**.
4. You should have the following information listed on your Window System:
 - **IP Address: 192.168.1.x**
 - **Submask: 255.255.255.0**
 - **Default Gateway IP: 192.168.1.1**

5. I forgot or lost my Administrator Password.

Ans. Reset the 4 Ports ADSL2/2+ Router to factory default by pressing the “**Reset**” button for 10 seconds.

If you are still getting prompted for a password when saving settings:

1. Access the Router's web interface by going to **http://192.1681.1**.
2. Enter the default “**username**” and “**password**” then click “**Enter**” to log in.
3. Click on “**TOOLS**” then click “**User Management**”.
4. Enter a new “**Password**” and new “**Username**” in the “**Username**” and “**Password**” field, and enter the same password in the second field to confirm the password.
5. Click “**Apply**” after your setting.

6. I need to upgrade the Firmware.

Ans. In order to upgrade the Firmware with the latest features, go to the PTI's website and download the latest Firmware at www.paradigm.com.tw. Before proceed the upgrading process, check the following details:

1. Download the latest Firmware and save at your pointed location.
2. Read the firmware release note carefully before proceed the upgrading process.
3. Refer to **TOOLS → Update Gateway** section for the upgrading process.

7. Testing LAN path to your 4 Ports ADSL2/2+ Router.

Ans. To verify whether the LAN path from your PC to your 4 Ports ADSL2/2+ Router is properly connected, you can “**Ping**” the 4 Ports ADSL2/2+ Router with the following procedures:

1. From the Windows toolbar, click “**Start**” and select “**Run**”.
2. In the open field, type “**Ping 192.168.1.1**” and click “**OK**”
3. If the path is working, you should see the message in the following format:
Reply from 192.168.1.1 bytes = 32 time < 10ms TTL = 60
4. If the path is not working, you should see the following message:
Request timed out

If the path is not functioning correctly:

1. Make sure the LAN port LED indicator is on.
2. Check whether you are using the correct LAN cable.
3. Check your Ethernet Adaptor installation and configurations.
4. Verify that the IP address for your 4 Ports ADSL2/2+ Router and your workstation are correct and that the addresses are on the same subnet.

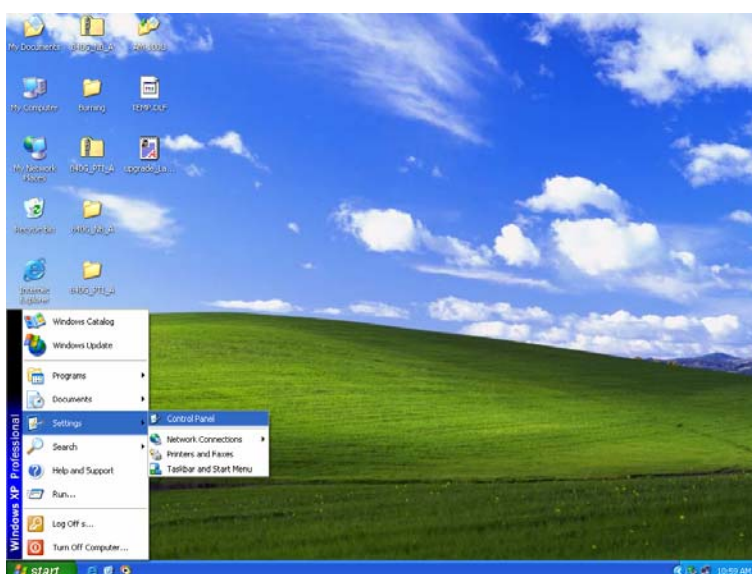
Appendix E: UPnP Setting on Windows XP

D.1 Adding UPnP:

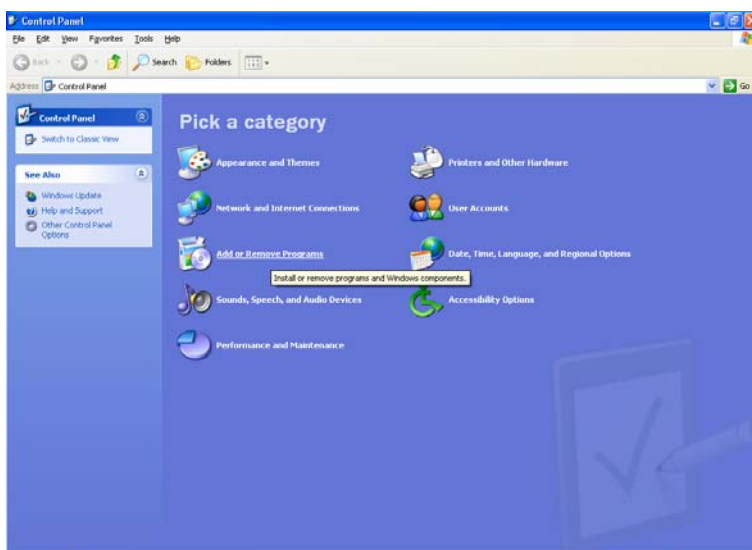
If you are running Microsoft Windows XP, it is recommended to add the UPnP component to your system.

Proceed as follows:

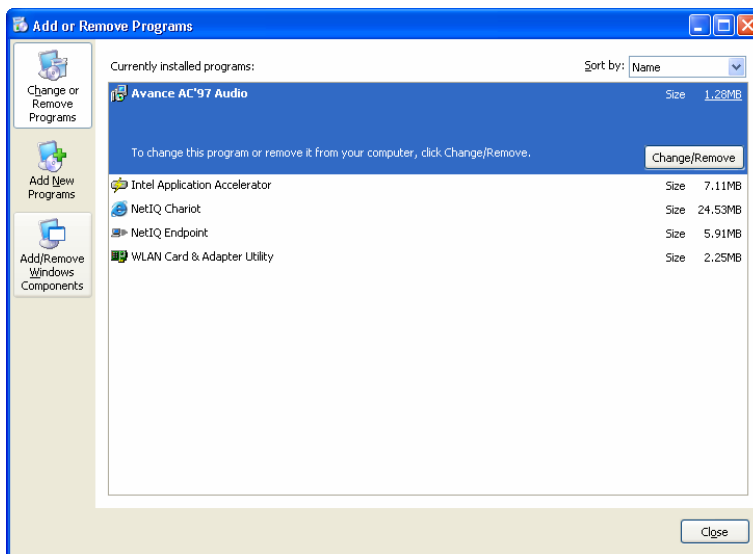
1. Click **“Start”** → **“Settings”** then **“Control Panel”**.



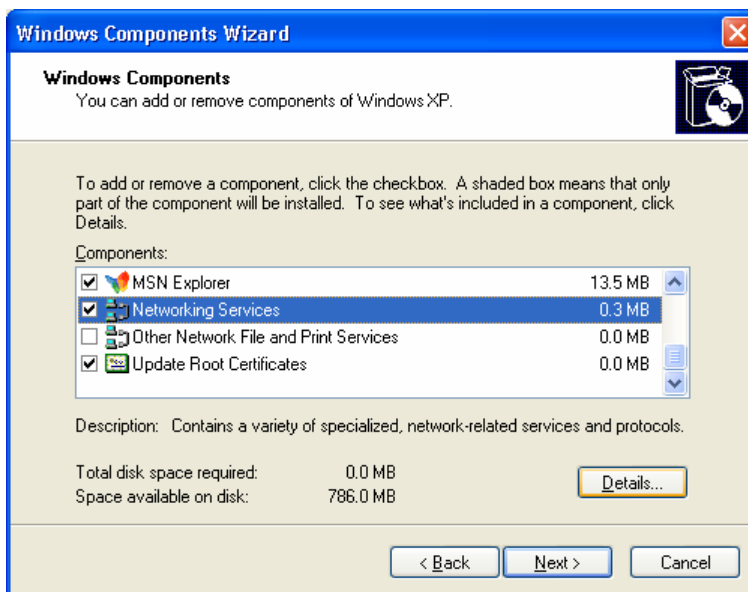
2. The **“Control Panel”** window appears. Click **“Add or Remove Programs”**.



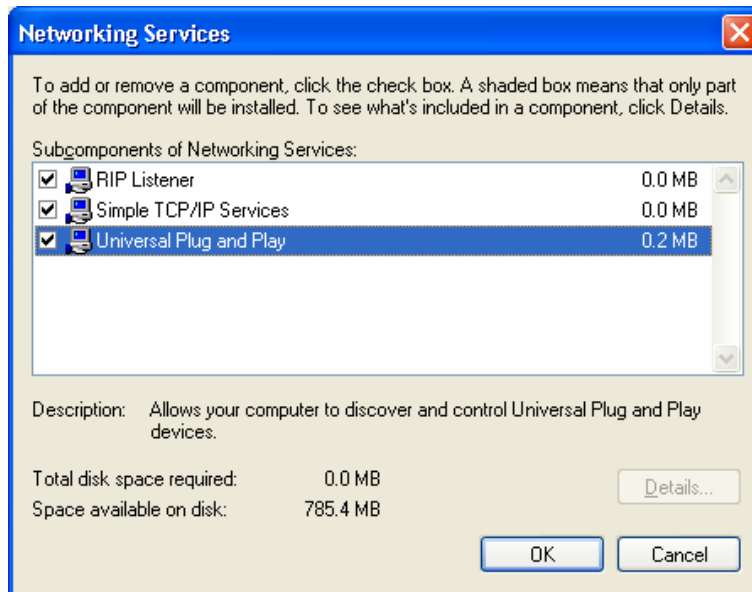
3. The “Add or Remove Programs” window appears. Click “Add/Remove Windows Components”.



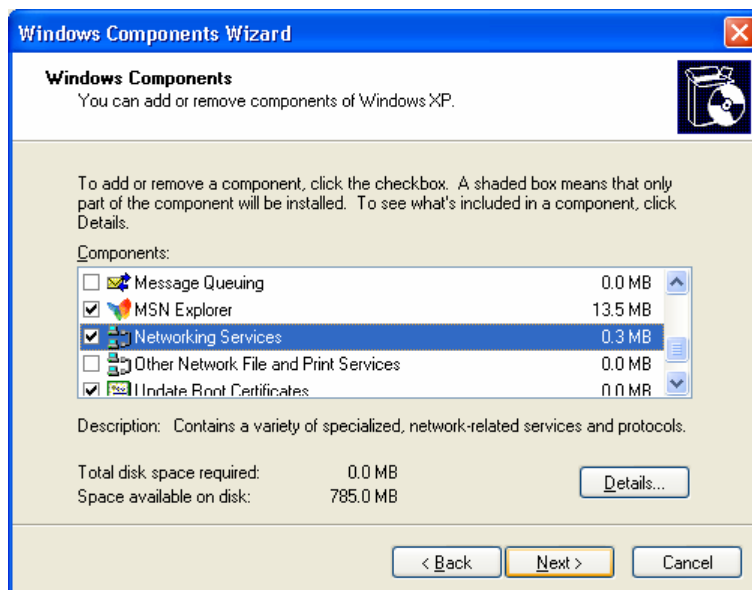
4. The “Windows Components Wizard” appears. Select “Networking Services” in the Components list and click “Details”.



5. The “Networking Services” window appears. Select “Universal Plug and Play” and click “OK”.



6. Click “Next” to start the installation and follow the instructions in the Windows Components Wizard.



Note : System may ask for original Windows XP CD-ROM. Insert the CD-ROM and direct Windows to the proper location of the CD-ROM.

**Restart your Windows system to activate your setting might be necessary.
Click “OK” to restart your Windows system.**

7. A “Completing the Windows Components Wizard” will appear indicating the installation was successful. Click “Finish” to quit.



Appendix F: Glossary

The Glossary provides an explanation of terms and acronyms discussed in this user guide.

10BASE-T: IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx: IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.11b: IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11g: IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11x: 802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys.

AP: Access Point: A station that transmits and receives data in a WLAN (Wireless Local Area Network). An access point acts as a bridge for wireless devices into a LAN.

ATM: Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

BC: Broadcast: Communication in which a sender transmits to everyone in the network.

BER: Bit Error Rate: Percentage of Bits that contain errors relative to the total number of bits transmitted.

Bridge: A device that connects two networks and decides which network the data should go to.

Bridge Mode: Bridge Mode is used when there is one PC connected to the LAN-side Ethernet or USB port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet or USB) side, i.e., to store and forward.

CBR: Constant Bit Rate: A constant transfer rate that is ideal for streaming (executing while still downloading) data, such as audio or video files.

Cell: A unit of transmission in ATM, consisting of a fixed-size frame containing a 5-octet header and a 48-octet payload.

CHAP: Challenge Handshake Authentication Protocol: Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

CLP: Cell Loss Priority: ATM cells have two levels of priority, CLP0 and CLP1. CLP0 is of higher priority, and in times of high traffic congestion, CLP1 error cells may be discarded to preserve the Cell Loss Ratio of the CLP0 cells.

CO: Central Office: In a local loop, a Central Office is where home and office phone lines come together and go through switching equipment to connect them to other Central Offices. The distance from the Central Office determines whether or not an ADSL signal can be supported in a given line.

CPE: Customer Premises Equipment. This specifies equipment on the customer, or LAN, side.

CRC: Cyclic Redundancy Checking: A method for checking errors in a data transmission between two computers. CRC applies a polynomial function (16 or 32-bit) to a block of data. The result of that polynomial is appended to the data transmission. Upon receipt, the destination computer applies the same polynomial to the block of data. If the host and destination computer share the same result, the transmission was successful. Otherwise, the sender is notified to re-send the data block.

DHCP: Dynamic Host Configuration Protocol: A communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP can lease an IP address or provide a permanent static address to those computers who need it (servers, etc.).

DMZ: Demilitarized Zone: A computer Host or network that acts as a neutral zone between a private network and a public network. A DMZ prevents users outside of the private network from getting direct access to a server or any computer within the private network. The outside user sends requests to the DMZ, and the DMZ initiates sessions in the public network based on these requests. A DMZ cannot initiate a session in the private network, it can only forward packets to the private network as they are requested.

DNS: Domain Name System: A method to locate and translate Domain Names into Internet Protocol (IP) addresses, where a Domain Name is a simple and meaningful name for an Internet address.

DSL: Digital Subscriber Line: A technology that provides broadband connections over standard phone lines.

DSLAM: Digital Subscriber Line Access Multiplexer: Using multiplexing techniques, a DSLAM receives signals from customer DSL lines and places the signals on a high-speed backbone line. DSLAMs are typically located at a telephone company's CO (Central Office).

Encapsulation: The inclusion of one data structure within another. For example, packets can be encapsulated in an ATM frame during transfer.

FEC: Forward Error Correction: An error correction technique in which a data packet is processed through an algorithm that adds extra error correcting bits to the packet. If the transmitted message is received in error, these bits are used to correct the errored bits without retransmission.

Firewall: A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Fragmentation: Breaking a packet up into smaller packets that is caused either by the transmission medium being unable to support the original size of the packet or the receiving computer not being able to receive a packet of that size. Fragmentation occurs when the sender's MTU is larger than the receiver's MRU.

FTP: File Transfer Protocol. A standardized internet protocol which is the simplest way to transfer files from one computer to another over the internet. FTP uses the Internet's TCP/IP protocols to function.

Full Duplex: Data transmission can be transmitted and received on the same signal medium and at the same time. Full Duplex lines are bidirectional.

G.dmt: Formally G.992.1, G.dmt is a form of ADSL that uses Discrete MultiTone (DMT) technology. G.dmt incorporates a splitter in its design.

G.lite: Formally G.992.2, G.lite is a standard way to install ADSL service. G.lite enables connections speeds up to 1.5 Mbps downstream and 128 kbps upstream. G.lite does not need a splitter at the user end because splitting is preformed at the remote end (telephone company).

Gateway: A point on the network which is an entrance to another network. For example, a router is a gateway that connects a LAN to a WAN.

Half Duplex: Data transmission can be transmitted and received on the same signal medium, but not simultaneously. Half Duplex lines are bidirectional.

HEC: Headed Error Control: ATM error checking by using a CRC algorithm on the fifth octet in the ATM cell header to generate a check character. Using HEC, either a single bit error in the header can be corrected or multiple bit errors in the header can be detected.

HNP: Home Network Processor

Host: In context of Internet Protocol, a host computer is one that has full two way access to other computers on the Internet.

IAD: Integrated Access Device: A device that multiplexes and demultiplexes communications in the CPE onto and out of a single telephone line for transmission to the CO.

IP: Internet Protocol: The method by which information is sent from one computer to another through the Internet. Each of these host computers have a unique IP address which distinguishes it from all the other computers on the internet. Each packet of data sent includes the sender's IP address and the receiver's IP address.

LAN: Local Area Network: A group of computers, typically covering a small geographic area, that share devices such as printers, hard disk drives, scanners, and optical drives. Computers in a LAN typically share an internet connection through some sort of router that connects the computers to a WAN.

LLC: Logical Link Control: Provides an interface point to the MAC sublayer. LLC Encapsulation is needed when several protocols are carried over the same Virtual Circuit.

MAC Address: Media Access Control Address: A unique hardware number on a computer or device that identifies it and relates it to the IP address of that device.

MC: Multicast: Communication involving a single sender and multiple specific receivers in a network.

MRU: Maximum Receive Unit: MRU: Maximum Receive Unit (MRU) is the largest size packet that can be received by the modem. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MSS: Maximum Segment Size: The largest size of data that TCP will send in a single, unfragmented IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their Maximum Segment Size during the TCP connection handshake.

MTU: Maximum Transmission Unit: The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

NAPT: Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

NAT: Network Address Translation: The translation of an IP address of one network to a different IP address known by another network. This gives an outside (WAN) network the ability to distinguish a device on the inside (LAN) network, as the inside network has a private set of IP address assigned by the DHCP server not known to the outside network.

PAP: Password Authentication Protocol: An authentication protocol in which authorization is done through a user name and password.

PDU: Protocol Data Unit: A frame of data transmitted through the data link layer 2.

Ping: Packet Internet Groper: A utility used to determine whether a particular device is online or connected to a network by sending test packets and waiting for a response.

PPP: Point-to-Point Protocol: A method of transporting and encapsulating IP packets between the user PC and the ISP. PPP is full duplex protocol that is transmitted through a serial interface.

Proxy: A device that closes a straight connection from an outside network (WAN) to an inside network (LAN). All transmissions must go through the proxy to get into or out of the LAN. This makes the internal addresses of the devices in the LAN private.

PVC: Permanent Virtual Circuit: A software defined logical connection in a network; A Virtual Circuit that is permanently available to the user.

RIP: Routing Information Protocol: A management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge.

RIPv1: RIP Version 1: One of the first dynamic routing protocols introduced used in the internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.

RIPv2: RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.

Router Mode: Router Mode is used when there is more than one PC connected to the LAN-side Ethernet and/or USB port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

SNAP: SubNetwork Attachment Point.

SNMP: Simple Network Management Protocol: Used to govern network management and monitor devices on the network. SNMP is formally described in RFC 1157.

SNR: Signal-to-Noise Ratio: Measured in decibels, SNR is a calculated ratio of signal strength to background noise. The higher this ratio, the better the signal quality.

Subnet Mask: Short for SubNetwork Mask, subnet mask is a technique used by the IP protocol to filter messages into a particular network segment, called a subnet. The subnet mask consists of a binary pattern that is stored in the client computer, server, or router. This pattern is compared with the incoming IP address to determine whether to accept or reject the packet.

TCP: Transfer Control Protocol: Works together with Internet Protocol for sending data between computers over the Internet. TCP keeps track of the packets, making sure that they are routed efficiently.

TFTP: Trivial File Transfer Protocol: A simple version of FTP protocol that has no password authentication or directory structure capability.

Trellis Code: An advanced method of FEC (Forward Error Correction). When enabled, it makes for better error checking at the cost of slower packet transmission. Setting Trellis Code to Disabled will cause increased packet transmission with decreased error correction.

TTL: Time To Live: A value in an IP packet that indicates whether or not the packet has been propagating through the network too long and should be discarded.

UBR: Unspecified Bit Rate: A transfer mode that is usually used in file transfers, email, etc. UBR can vary depending on the data type.

USB: Universal Serial Bus: A standard interface between a computer and a peripheral (printer, external drives, digital cameras, scanners, network interface devices, modems, etc.) that allows a transfer rate of 12Mbps.

UDP: User Datagram Protocol: A protocol that is used instead of TCP when reliable delivery is not required. Unlike TCP, UDP does not require an acknowledgement (handshake) from the receiving end. UDP sends packets in one-way transmissions.

VBR-nrt: Variable Bit Rate – non real time: With VBR-nrt, cell transfer is variable upon certain criteria.

VC: Virtual Circuit: A virtual circuit is a circuit in a network that appears to be a physically discrete path, but is actually a managed collection of circuit resources that allocates specific circuits as needed to satisfy traffic requirements.

VCI: Virtual Channel Identifier: A virtual channel identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel.

VC-Mux: Virtual Circuit based Multiplexing: In VC Based Multiplexing, the interconnect protocol of the carried network is identified implicitly by the VC (Virtual Circuit) connecting the two ATM stations (each protocol must be carried over a separate VC).

VPI:Virtual Path Identifier: Virtual path for cell routing indicated by an eight bit field in the ATM cell header.

WAN: Wide Area Network: A WAN covers a large geographical area. A WAN is consisted of LANs and the Internet is consisted of WANs.

WPA: Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.